Arcserve® Unified Data Protection Agent for Linux

Benutzerhandbuch

Version 5.0

arcserve®

Diese Dokumentation, die eingebettete Hilfssysteme und elektronisch verteilte Materialien beinhaltet (im Folgenden als "Dokumentation" bezeichnet), dient ausschließlich zu Informationszwecken des Nutzers und kann von Arcserve jederzeit geändert oder zurückgenommen werden. Diese Dokumentation stellt geistiges Eigentum von Arcserve dar und darf ohne vorherige schriftliche Genehmigung von Arcserve weder vollständig noch auszugsweise kopiert, übertragen, vervielfältigt, veröffentlicht, geändert oder dupliziert werden.

Der Benutzer, der über eine Lizenz für das bzw. die in dieser Dokumentation berücksichtigten Software-Produkt(e) verfügt, ist dazu berechtigt, eine angemessene Anzahl an Kopien dieser Dokumentation zum eigenen innerbetrieblichen Gebrauch im Zusammenhang mit der betreffenden Software auszudrucken oder anderweitig verfügbar zu machen, vorausgesetzt, dass jedes Exemplar diesen Urheberrechtsvermerk und sonstige rechtliche Hinweise von Arcserve enthält.

Dieses Recht zum Drucken oder anderweitigen Anfertigen einer Kopie der Dokumentation beschränkt sich auf den Zeitraum der vollen Wirksamkeit der Produktlizenz. Sollte die Lizenz aus irgendeinem Grund enden, bestätigt der Lizenznehmer gegenüber Arcserve schriftlich, dass alle Kopien oder Teilkopien der Dokumentation an Arcserve zurückgegeben oder vernichtet worden sind.

SOWEIT NACH ANWENDBAREM RECHT ERLAUBT, STELLT ARCSERVE DIESE DOKUMENTATION IM VORLIEGENDEN ZUSTAND OHNE JEGLICHE GEWÄHRLEISTUNG ZUR VERFÜGUNG; DAZU GEHÖREN INSBESONDERE STILLSCHWEIGENDE GEWÄHRLEISTUNGEN DER MARKTTAUGLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET ARCSERVE GEGENÜBER IHNEN ODER DRITTEN GEGENÜBER FÜR VERLUSTE ODER UNMITTELBARE ODER MITTELBARE SCHÄDEN, DIE AUS DER NUTZUNG DIESER DOKUMENTATION ENTSTEHEN; DAZU GEHÖREN INSBESONDERE ENTGANGENE GEWINNE, VERLORENGEGANGENE INVESTITIONEN, BETRIEBSUNTERBRECHUNG, VERLUST VON GOODWILL ODER DATENVERLUST, SELBST WENN ARCSERVE ÜBER DIE MÖGLICHKEIT DIESES VERLUSTES ODER SCHADENS INFORMIERT WURDE.

Der Gebrauch jedes einzelnen der in der Dokumentation genannten Softwareprodukte unterliegt dem geltenden Lizenzabkommen, und dieses Lizenzabkommen wird durch die Bedingungen dieses Hinweises in keiner Weise geändert.

Der Hersteller dieser Dokumentation ist Arcserve.

Es gelten "Eingeschränkte Rechte". Die Verwendung, Vervielfältigung oder Veröffentlichung durch die Regierung der Vereinigten Staaten unterliegt den jeweils in den FAR-Abschnitten 12.212, 52.227-14 und 52.227-19(c)(1) - (2) sowie dem DFARS-Abschnitt 252.227-7014(b)(3) oder in ihren Nachfolgeabschnitten festgelegten Einschränkungen.

Copyright © 2015 Arcserve (USA), LLC und seine Schwestergesellschaften und Tochtergesellschaften. Alle Rechte vorbehalten. Alle Markenzeichen, Markennamen, Dienstleistungsmarken und Logos, auf die hier verwiesen wird, sind Eigentum der jeweiligen Unternehmen.

Arcserve-Support kontaktieren

Das Arcserve-Support-Team stellt umfangreiche Ressourcen zur Lösung von technischen Problemen zur Verfügung und bietet einfachen Zugriff auf wichtige Produktinformationen.

http://www.arcserve.com/de/default.aspx

Mit Arcserve-Support:

- Sie können direkt auf dieselbe Informationsbibliothek zugreifen, die auch intern von Arcserve-Support-Fachleuten verwendet wird. Diese Website bietet Zugriff auf unsere Knowledge Base-Dokumente (KB-Dokumente). Hier können Sie schnell und einfach produktbezogene KB-Artikel suchen und aufrufen, die praxiserprobte Lösungen für viele häufig auftretende Probleme enthalten.
- Sie können unseren Live-Chat-Link verwenden, um sofort ein Echtzeitgespräch mit dem Team für Arcserve-Support zu starten. Über den Live-Chat können Bedenken und Fragen bei noch bestehendem Zugriff auf das Produkt umgehend behandelt werden.
- Sie können sich an der globalen Benutzer-Community von Arcserve beteiligen, um Fragen zu stellen und zu beantworten, Tipps und Tricks zu weiterzugeben, Best Practices zu diskutieren und sich mit Gleichgesinnten zu unterhalten.
- Sie können Support-Tickets erstellen. Wenn Sie ein Online-Support-Ticket öffnen, wird Sie ein Experte aus dem betroffenen Produktbereich zurückrufen.
- Sie können auf weitere hilfreiche Ressourcen für Ihr Arcserve-Produkt zugreifen.

Inhalt

Kapitel 1: Funktionsweise von Arcserve UDP Agent (Linux) 9

Einführung 9

Kapitel 2: Installieren bzw. Deinstallieren von Arcserve UDP Agent (Linux) 13

So installieren Sie Arcserve UDP Agent (Linux) 13
- Installationshinweise 14
- Installieren von Arcserve UDP Agent (Linux) 14
- Überprüfen der Installation 17

So deinstallieren Sie Arcserve UDP Agent (Linux) 18
- Lesen der Hinweise zur Deinstallation 19
- Deinstallieren von Arcserve UDP Agent (Linux) 19
- Überprüfen der Deinstallation 19

So führen Sie ein Upgrade von Arcserve UDP Agent (Linux) aus 20
- Zu Aktualisierungen 20
- Durchführen eines Upgrades von Arcserve UDP Agent (Linux) 21
- Überprüfen des Upgrade 23

Kapitel 3: Benutzeroberfläche 25

So navigieren Sie in der Benutzeroberfläche von Arcserve UDP Agent (Linux) 25
- Zugreifen auf den Sicherungsserver 27
- Kennenlernen der Menüleiste 27
- Kennenlernen des Statusfensters 30
- Kennenlernen des Sicherungsserver-Fensters 34
- Kennenlernen der Hilfe 35

Kapitel 4: Verwenden von Arcserve UDP Agent (Linux) 37

So verwalten Sie die Lizenzen 37
- Zugriff auf den Lizenzmanager 38
- Funktionsweise des Dialogfeldes "Lizenzverwaltung" 39
- Verwalten der Lizenzen 40

So verwalten Sie Jobs 41
- Überprüfen der Voraussetzungen zur Verwaltung von Jobs 42
- Ändern von Jobs 42
- Abbrechen von Jobs 42
- Löschen von Jobs 43

So sichern Sie Linux-Knoten 44
Überprüfen der Voraussetzungen und Hinweise für Sicherungen 45
Sichern von mehr als 200 Knoten 47
Hinzufügen von Linux-Knoten zur Sicherung 50
(Optional) Vorbereiten des iSCSI-Volume als Sicherungsspeicher 53
Konfigurieren der Sicherungseinstellungen und erneutes Ausführen des Sicherungsjobs 54
Überprüfen, ob die Sicherung erfolgreich ausgeführt wurde 76
So ändern Sie einen Sicherungsjob und führen ihn erneut aus 76
Überprüfen der Voraussetzungen für das Ändern eines Sicherungsjobs 78
Möchten Sie Knoten zu einem vorhandenen Job hinzufügen? 78
Hinzufügen von Knoten zu einem vorhandenen Job 78
Erneutes Ausführen eines vorhandenen Sicherungsjobs 79
Überprüfen, ob die Sicherung erfolgreich ausgeführt wurde 80
So führen Sie eine Wiederherstellung der Dateiebene unter Linux-Knoten aus 80
Überprüfen der Voraussetzungen 82
(Optional) Wiederherstellen von Daten des iSCSI-Volume des Zielcomputers 83
Angeben des Wiederherstellungspunkts 84
Angeben der Details des Zielcomputers 88
Festlegen von erweiterten Einstellungen 92
Erstellen und Ausführen des Wiederherstellungsjobs 96
Überprüfen, dass Dateien wiederhergestellt wurden 97
So erstellen Sie eine startfähige Live-CD 98
Überprüfen der Voraussetzungen für Live-CD 99
Installieren des Wiederherstellungs-Hilfsprogrammpakets 100
Erstellen und Überprüfen der startfähigen Live-CD 100
So erstellen Sie eine CentOS-basierte Live-CD 102
Überprüfen der Voraussetzungen und Hinweise für Live-CDs 103
Installieren des Wiederherstellungs-Hilfsprogrammpakets 105
Erstellen und Überprüfen der CentOS-basierten Live-CD 105
So führen Sie eine Bare-Metal-Recovery (BMR) für Linux-Rechner aus 106
Überprüfen der Voraussetzungen 109
Abrufen der IP-Adresse des Zielcomputers mithilfe der Live-CD 110
(Optional) Wiederherstellen von Daten auf dem iSCSI-Volume des Zielcomputers 111
(Optional) Wiederherstellen von Daten des iSCSI-Volume des Zielcomputers 112
Überprüfen des Sicherungsservers 113
Angeben der Wiederherstellungspunkte 114
Angeben der Details des Zielcomputers 117
Festlegen von erweiterten Einstellungen 117
Erstellen und Ausführen des Wiederherstellungsjobs 122
Überprüfen, dass der Zielknoten wiederhergestellt wurde 129
So stellen Sie einen virtuellen Rechner automatisch wieder her 130
Überprüfen der Voraussetzungen und Hinweise 132

Erstellen einer Konfigurationsvorlage 135
(Optional) Erstellen einer globalen Konfigurationsdatei 139
Ändern der Konfigurationsvorlage und -datei 141
Senden eines Jobs mithilfe des d2drestorevm-Hilfsprogramms 141
Überprüfen der VM-Wiederherstellung 142
So integrieren und automatisieren Sie Arcserve Unified Data Protection Agent for Linux in einer bestehenden IT-Umgebung 142
Überprüfen der Voraussetzungen für die Automatisierung 144
Kennenlernen der Skripterstellungs-Hilfsprogramme 145
Verwalten der Prä-/Post-Skripte für Automatisierung 156
Erstellen von Skripts für Sicherungsspeicher-Alert 159
Ermitteln von Knoten mit einem Skript 159
Erstellen von Skripten, um die Oracle-Datenbank zu sichern 161
Erstellen von Skripten, um die MySQL-Datenbank zu sichern 163
Anpassen des Job-Ablaufplans 165
Ausführen eines BMR-Batch-Jobs 166
Replizieren und Verwalten von Sicherungssitzungen 168
Überprüfen, ob die Wiederherstellungspunkte verwendet werden können 171
So verwalten Sie die Einstellungen des Sicherungsservers 177
Überprüfen der Voraussetzungen zur Verwaltung des Sicherungsservers 179
Konfigurieren der Aufbewahrungseinstellungen des Jobverlaufs und der Aktivitätsprotokolle 179
Konfigurieren der Aufbewahrungseinstellungen des Debug-Protokolls 180
Konfigurieren der Zeitüberschreitungsdauer der Benutzeroberfläche 181
Ändern der SSH-Portnummer des Sicherungsservers 181
Verwalten der Wiederherstellungssätze 182
Deaktivieren der Dienste "BOOTPD" und "TFTPD" 183
Verbessern der Abfrageleistung für Jobverlauf und Aktivitätsprotokoll 183
Überspringen der Prüfung von CIFS- und NFS-Clients 184
So verwalten Sie einen Linux-Sicherungsserver über die Befehlszeile 185
Überprüfen der Voraussetzungen für den Sicherungsserver 186
Starten, Anhalten oder Freigeben des Sicherungsservers 187
Ändern der Webservice-Portnummer des Sicherungsservers 188
Konfigurieren der Authentifizierung mit privatem und öffentlichem Schlüssel 189
Ändern des Sicherungsserverprotokolls 190
Vermeiden des SSL-Zertifikatsfehlers beim Öffnen von Arcserve UDP Agent (Linux) 191
Konfigurieren der Systemeinstellungen, wenn der Hostname oder die IP-Adresse geändert wurde 193
So verwalten Sie Nicht-Root-Benutzer 198
Überprüfen der Voraussetzungen 199
Gewähren von Anmeldeberechtigungen für Nicht-Root-Benutzer 199
Anzeigen des Standardbenutzers im Anmeldedialogfeld 200
Aktivieren der Nicht-Root-Benutzer, um Knoten hinzuzufügen 201
So stellen Sie Volumes auf einem Zielknoten wieder her 202

Überprüfen der Voraussetzungen und Hinweise 204
Überprüfen, ob das Hilfsprogramm "d2drestorevol" installiert ist 205
Überprüfen der Volume-Details in der Sitzung 206
Übergeben des Volume-Wiederherstellungsjobs 207
Abbrechen des Volume-Wiederherstellungsjobs 210
Überprüfen des wiederhergestellten Volumes 210
So stellen Sie eine Oracle-Datenbank mithilfe von Arcserve UDP Agent (Linux) wieder her 211
Ausführen einer Bare-Metal-Recovery (BMR) eines Oracle-Servers 213
Ausführen einer sofortigen Wiederherstellung einer Oracle-Datenbank 215
Ausführen einer spezifischen Wiederherstellung einer Oracle-Datenbank 217

Kapitel 5: Fehlerbehebung 223

Kapitel 1: Funktionsweise von Arcserve UDP Agent (Linux)

Dieses Kapitel enthält folgende Themen:

Einführung (siehe Seite 9)

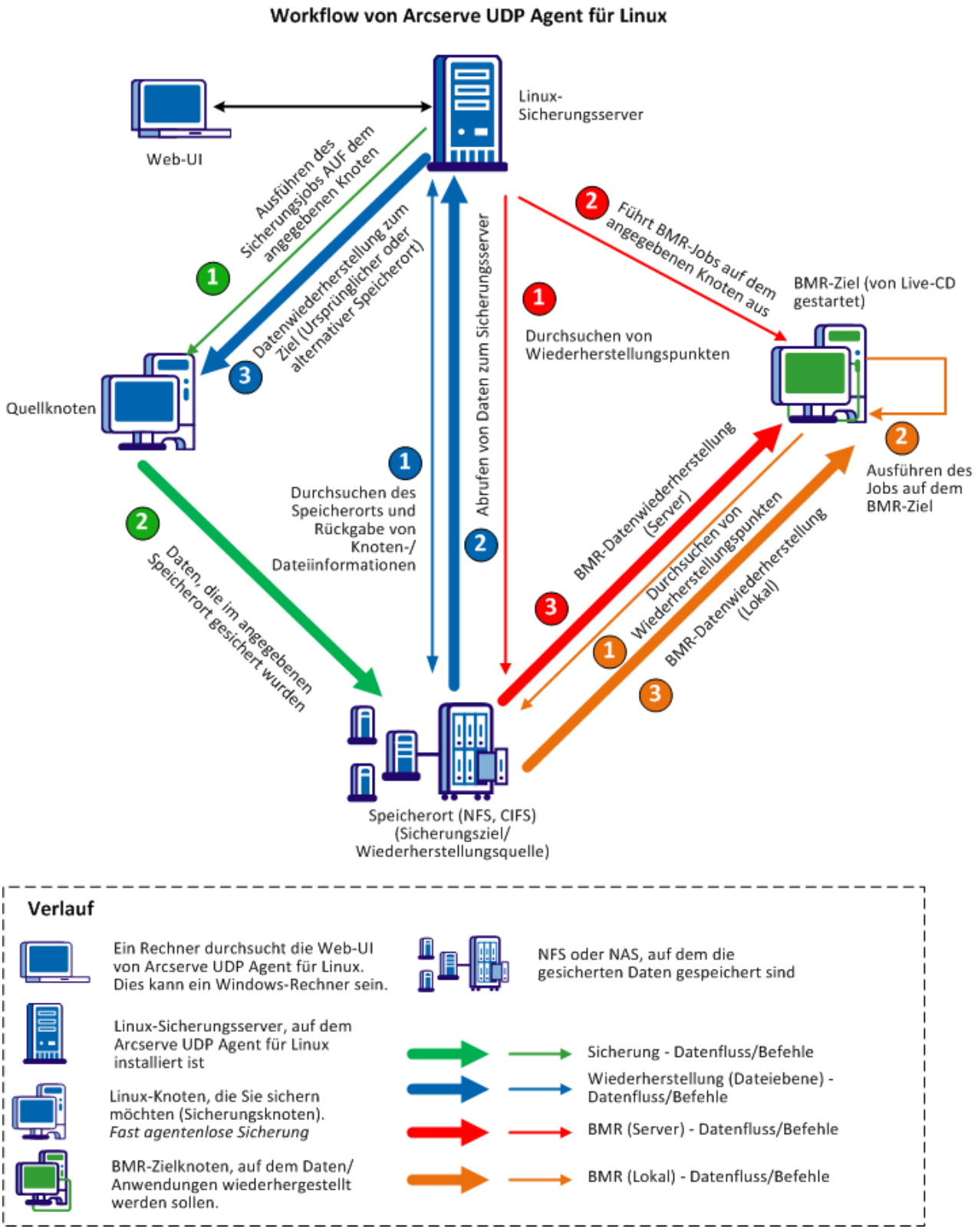
Einführung

Arcserve Unified Data Protection Agent for Linux (Arcserve UDP Agent (Linux)) ist ein datenträgerbasiertes Sicherungsprodukt, das für Linux-Betriebssysteme entworfen wurde. Es bietet eine schnelle, einfache und zuverlässige Möglichkeit zum Schützen und Wiederherstellen von wichtigen Unternehmensdaten. Arcserve UDP Agent (Linux) verfolgt Änderungen in Knoten auf Blockebene und sichert nur die geänderten Blöcke in einem inkrementellen Vorgang. Dadurch ermöglicht Arcserve UDP Agent (Linux) häufige Sicherungen. Die Größe der einzelnen Zuwachssicherungen reduziert sich (und damit auch das Zeitfenster für die Sicherung), und der Status der Sicherungen ist aktueller. Zusätzlich verfügt Arcserve UDP Agent (Linux) über eine Funktion zur Wiederherstellung von Dateien oder Ordnern sowie zur Bare-Metal-Recovery (BMR) einzelner Sicherungen. Sie können die Sicherungsinformationen auch auf einer NFS-Freigabe (Network File System), einer CIFS-Freigabe (Common Internet File System) oder im Sicherungsquellknoten speichern.

Eine BMR ist der Prozess, bei dem ein *Bare-Metal*-Computersystem wiederhergestellt wird. "Bare Metal" bezeichnet einen Computer ohne Betriebssystem, Treiber und Software-Anwendungen. Die Wiederherstellung umfasst die Installation des Betriebssystems, der Software-Anwendungen und Treiber sowie die anschließende Wiederherstellung der Daten und Einstellungen. Eine BMR ist möglich, da Arcserve UDP Agent (Linux) beim Ausführen einer Sicherung von Daten auch Informationen zu Betriebssystem, installierten Anwendungen, Treibern usw. aufzeichnet. Nachdem eine BMR ausgeführt wurde, verfügt der Zielknoten über das gleiche Betriebssystem und die gleichen Daten wie der Produktionsknoten.

Arcserve UDP Agent (Linux) verwendet für den schnellen und flexiblen Schutz aller Linux-Clients eine fast agentenlose Methode. Diese Funktion macht die Notwendigkeit, Agents manuell auf jedem Client-Knoten zu installieren, völlig überflüssig, und automatisiert die Erkennung, Konfiguration und den Schutz aller Ihrer Linux-Clients dadurch vollständig. Die Installation von Arcserve UDP Agent (Linux) ist hilfreich, um die gesamte Linux-Produktionsumgebung zu schützen. Der Server, auf dem Sie Arcserve UDP Agent (Linux) installieren, wird als Sicherungsserver bezeichnet. Nachdem Sie Arcserve UDP Agent (Linux) installiert haben, können Sie über ein Netzwerk eine Verbindung mit dem Sicherungsserver herstellen und die Benutzeroberfläche in einem Webbrowser öffnen.

Das folgende Diagramm veranschaulicht den gesamten Workflow von Arcserve UDP Agent (Linux):


Workflow von Arcserve UDP Agent für Linux
Linux-
Sicherungsserver
Web-UI
Ausführen des
Sicherungsjobs AUF dem
angegebenen Knoten
Datenwiederherstellung zum
Ziel (Ursprünglicher oder
alternativer Speicherort)
Führt BMR-Jobs auf dem
angegebenen Knoten aus
BMR-Ziel (von Live-CD
gestartet)
Durchsuchen von
Wiederherstellungspunkten
Quellknoten
Abrufen von Daten zum Sicherungsserver
Durchsuchen des
Speicherorts und
Rückgabe von
Knoten-/
Dateiinformationen
Daten, die im angegebenen
Speicherort gesichert wurden
BMR-Datenwiederherstellung
(Server)
Durchsuchen von
Wiederherstellungspunkten
BMR-Datenwiederherstellung
(Lokal)
Ausführen des
Jobs auf dem
BMR-Ziel
Speicherort (NFS, CIFS)
(Sicherungsziel/
Wiederherstellungsquelle)
Verlauf
Ein Rechner durchsucht die Web-UI
von Arcserve UDP Agent für Linux.
Dies kann ein Windows-Rechner sein.
NFS oder NAS, auf dem die
gesicherten Daten gespeichert sind
Linux-Sicherungsserver, auf dem
Arcserve UDP Agent für Linux
installiert ist
Linux-Knoten, die Sie sichern
möchten (Sicherungsknoten).
Fast agentenlose Sicherung
BMR-Zielknoten, auf dem Daten/
Anwendungen wiederhergestellt
werden sollen.
Sicherung - Datenfluss/Befehle
Wiederherstellung (Dateiebene) -
Datenfluss/Befehle
BMR (Server) - Datenfluss/Befehle
BMR (Lokal) - Datenfluss/Befehle

Kapitel 2: Installieren bzw. Deinstallieren von Arcserve UDP Agent (Linux)

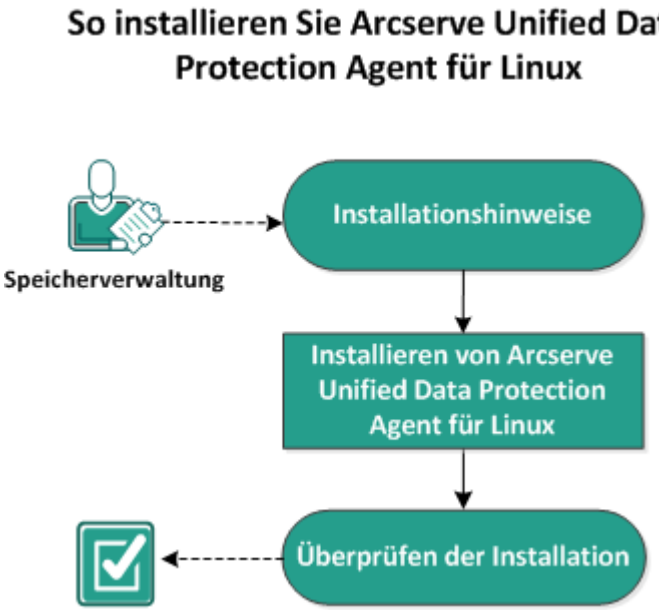
Dieses Kapitel enthält folgende Themen:

So installieren Sie Arcserve UDP Agent (Linux) (siehe Seite 13)
So deinstallieren Sie Arcserve UDP Agent (Linux) (siehe Seite 18)
So führen Sie ein Upgrade von Arcserve UDP Agent (Linux) aus (siehe Seite 20)

So installieren Sie Arcserve UDP Agent (Linux)

Installieren Sie Arcserve UDP Agent (Linux) auf einem Linux-Server, um alle Ihre Sicherungsquellknoten über eine einzige Benutzeroberfläche zu schützen und zu verwalten. Es ist nicht erforderlich, diese Software auf den Sicherungsquellknoten zu installieren.

Folgendes Diagramm zeigt den Installationsvorgang für Arcserve UDP Agent (Linux):


So installieren Sie Arcserve Unified Data Protection Agent für Linux
Speicherverwaltung
Installationshinweise
Installieren von Arcserve Unified Data Protection Agent für Linux
Überprüfen der Installation

Gehen Sie wie folgt vor, um Arcserve UDP Agent (Linux) zu installieren:

- Installieren von Arcserve UDP Agent (Linux) (siehe Seite 14)
- Überprüfen der Installation (siehe Seite 17)
- Installationshinweise (siehe Seite 14)

Installationshinweise

Beachten Sie Folgendes, bevor Sie mit der Installation beginnen:

- Wenn Sie eine PXE-BMR (Preboot Execution Environment) ausführen, müssen sich der Arcserve Unified Data Protection Agent for Linux-Server und die Produktionsquellknoten in demselben Subnetz befinden. Wenn sie sich nicht in demselben Subnetz befinden, stellen Sie sicher, dass ein Gateway vorhanden ist, mit dem die PXE-Übertragungspakete über die Subnetzen hinweg weitergeleitet werden.
- Wenn das Sicherungsziel ein NFS-Server ist, stellen Sie sicher, dass der NFS-Server das *Sperren* unterstützt. Stellen Sie außerdem sicher, dass der root-Benutzer über Schreibzugriff für die Linux-Knoten verfügt.
- Um einen NFS-Server als Sicherungsziel zu verwenden, installieren Sie das NFS-Client-Paket auf den Linux-Knoten.
- Perl und sshd (SSH-Daemon) sind auf dem Linux-Server und auf den Knoten installiert, die Sie sichern möchten.
- Die unbeaufsichtigte oder automatische Installation wird nicht unterstützt.
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Installieren von Arcserve UDP Agent (Linux)

Installieren Sie Arcserve UDP Agent (Linux) auf einem Linux-Server, um Sicherungs- und Wiederherstellungsvorgänge zu verwalten. Nachdem Sie Arcserve UDP Agent (Linux) installiert haben, können Sie die Benutzeroberfläche von einem Computer mithilfe eines Webbrowsers öffnen und der Server wird als Sicherungsserver verwiesen.

Bei Beginn der Installation überprüft das Installationsskript, ob einige der obligatorischen Anwendungen auf dem Sicherungsserver installiert sind und ob die Anwendungen ausgeführt werden.

Folgende obligatorische Anwendungen sind erforderlich, damit die Installationsdatei funktioniert:

- sshd (SSH-Daemon)
- Perl

Die Installationsdatei überprüft bei Beginn der Installation auch folgende optionale Anwendungen:

- rpc.statd - Diese Anwendung wird vom NFS-Server verwendet, um die Dateisperre zu implementieren.
- mkisofs - Arcserve UDP Agent (Linux) verwendet diese Anwendung, um eine Live-CD zu erstellen.
- mount.nfs - Arcserve UDP Agent (Linux) verwendet diese Anwendung, um den NFS-Server zu laden.
- mount.cifs - Arcserve UDP Agent (Linux) verwendet diese Anwendung, um den CIFS-Server zu laden.
- ether-wake - Arcserve UDP Agent (Linux) verwendet diese Anwendung, um die Wake-on-Lan-Anforderung zu senden.

Hinweis: Stellen Sie sicher, dass der Sicherungsserver über mindestens 1 GB Arbeitsspeicher verfügt. Hinweis: Weitere Informationen zu den Systemanforderungen für einen Linux-Server finden Sie in den *Versionshinweisen*.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Linux-Server an.
2. Laden Sie das Arcserve UDP Agent (Linux)-Installationspaket (*.bin-Datei) und die Paketdatei mit dem Wiederherstellungshilfsprogramm in den Stammordner herunter.

   Wichtig! Wenn Sie die zwei Dateien des Installationspakets in einen lokalen Ordner herunterladen, dann darf der vollständige Pfad dieses lokalen Ordners keine Sonderzeichen (mit Ausnahme von Leerzeichen) enthalten, und der Pfad sollte nur folgende Zeichen umfassen: a-z, A-Z, 0-9, - und _.
3. Geben Sie dem Installationspaket Ausführungsberechtigungen.

4. Führen Sie einen der folgenden Schritte je nach Speicherort des Installationspakets und des Wiederherstellungs-Hilfsprogrammpakets aus:

   - Wenn das Installationspaket und das Wiederherstellungs-Hilfsprogrammpaket im gleichen Ordner sind, dann führen Sie folgenden Befehl aus, um die Installation zu beginnen:

     ```
     ./<linux_installation_file_name>.bin
     ```

     Hinweis: Wenn Sie das Paket mit dem Wiederherstellungshilfsprogramm umbenennen, dann muss der Paketname die Zeichen des Wiederherstellungshilfsprogramms enthalten, damit der Installationsbefehl das Paket mit dem Wiederherstellungshilfsprogramm automatisch findet und installiert. Wenn der Paketname die Zeichen des Wiederherstellungshilfsprogramms nicht enthält, müssen Sie den vollständigen Pfad des Pakets mit dem Wiederherstellungshilfsprogramm angeben.

     Das Installationspaket überprüft die unterstützte Plattform und zeigt eine Bestätigungsmeldung an.

     Wenn eine nicht unterstützte Plattform erkannt wird, tippen Sie "Y" und drücken Sie die Eingabetaste, um die Installation der nicht unterstützten Plattform zu bestätigen.

   - Wenn das Installationspaket und das Paket mit dem Wiederherstellungshilfsprogramm sich in verschiedenen Ordnern befinden, dann geben Sie den Pfad des Pakets mit dem Wiederherstellungshilfsprogramm im ersten Parameter an:

     ```
     ./<Linux_Installationsdateiname>.bin
     –-path=/<Pfad_des_Pakets_mit_dem_Wiederherstellungshilfsprogramm>
     ```

     Das Installationspaket überprüft die unterstützte Plattform und zeigt eine Bestätigungsmeldung an.

     Wenn eine nicht unterstützte Plattform erkannt wird, tippen Sie "Y" und drücken Sie die Eingabetaste, um die Installation der nicht unterstützten Plattform zu bestätigen.

   Hinweis: Wenn ein nicht-englisches Betriebssystem entdeckt wird, werden Sie aufgefordert, die anwendbare Sprache auszuwählen, bevor Sie mit dem Installationsprozess fortfahren.

5. Geben Sie "J" ein, und drücken Sie die Eingabetaste, um die Installation zu bestätigen.

   Das Installationspaket zeigt die Informationen zur Lizenzierungsvereinbarung an.

6. Geben Sie "J" ein, und drücken Sie die Eingabetaste, um die Lizenzierungsvereinbarung zu akzeptieren.

   Der Arcserve UDP Agent (Linux)-Installationsprozess beginnt.

   Wenn die Installation des Pakets mit dem Wiederherstellungshilfsprogramm abgeschlossen ist, werden die Live-CD-Build-Informationen angezeigt.

   Die Live-CD wird am folgenden Speicherort erzeugt:

   `/opt/CA/d2dserver/packages`

   Hinweis: Live-CD ist erforderlich, um die IP-Adresse des Zielknotens abzurufen, wenn Sie eine Bare-Metal-Recovery (BMR) ausführen.

   Arcserve UDP Agent (Linux) wird installiert, und die URL für den Linux-Sicherungsserver wird angezeigt.

   Hinweis: Stellen Sie sicher, dass folgende eingehende Ports auf Ihrer Firewall für den Sicherungsserver aktiviert sind:

   - TCP-Port 22 (SSH-Server)
   - Broadcast-Port 67 (Startserver)
   - 8014 (Agent-Webservice)
   - User Datagram Protocol (UDP) Port 69 (TFTP Server)

   Stellen Sie sicher, dass der folgende eingehende Port auf Ihrer Firewall für die Client-Knoten, die Sie sicherstellen möchten, aktiviert ist:

   - TCP-Port 22 (SSH-Server)

   Stellen Sie sicher, dass der erforderliche ausgehende Port für NFS, CIFS oder beide Sicherungsziele auf Ihrer Firewall für den Linux-Sicherungsserver und die Client-Knoten aktiviert sind.

Arcserve UDP Agent (Linux) wurde erfolgreich installiert.

Überprüfen der Installation

Überprüfen Sie nach der Installation von Arcserve UDP Agent (Linux), dass die Installation abgeschlossen ist.

Gehen Sie wie folgt vor:

1. Öffnen Sie auf einem Windows-Computer einen Webbrowser.
2. Geben Sie die URL des Linux-Sicherungsservers ein, die auf dem Installationsbildschirm angezeigt wird.

   Beispiel: https://hostname:8014

Die Anmeldeseite von Arcserve UDP Agent (Linux) wird geöffnet.

3. Geben Sie Ihre root-Anmeldeinformationen ein, und klicken Sie auf "Anmelden".

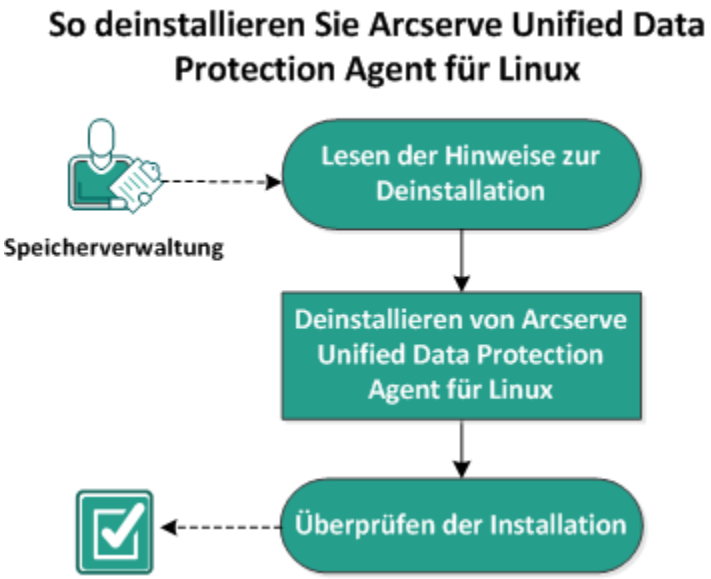
   Die Arcserve UDP Agent (Linux)-Benutzeroberfläche wird geöffnet.

Arcserve UDP Agent (Linux) wurde erfolgreich installiert und überprüft.

So deinstallieren Sie Arcserve UDP Agent (Linux)

Deinstallieren Sie Arcserve UDP Agent (Linux) vom Linux-Sicherungsserver, um den Schutz aller Knoten zu beenden.

Folgendes Flussdiagramm zeigt den Deinstallationsprozess für Arcserve UDP Agent (Linux):


So deinstallieren Sie Arcserve Unified Data Protection Agent für Linux
Speicherverwaltung
Lesen der Hinweise zur Deinstallation
Deinstallieren von Arcserve Unified Data Protection Agent für Linux
Überprüfen der Installation

Gehen Sie wie folgt vor, um Arcserve UDP Agent (Linux) zu deinstallieren:

- Lesen der Hinweise zur Deinstallation (siehe Seite 19)
- Deinstallieren von Arcserve UDP Agent (Linux) (siehe Seite 19)
- Überprüfen der Deinstallation (siehe Seite 19)

Lesen der Hinweise zur Deinstallation

Beachten Sie Folgendes, bevor Sie mit der Deinstallation beginnen:

- Sie verfügen über die root-Anmeldeinformationen für den Sicherungsserver.
- Es werden derzeit keine Jobs ausgeführt. Wenn ein Job ausgeführt wird, können Sie Arcserve UDP Agent (Linux) nicht deinstallieren.
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Deinstallieren von Arcserve UDP Agent (Linux)

Sie können Arcserve UDP Agent (Linux) über die Befehlszeile des Sicherungsservers deinstallieren. Bei der Deinstallation werden alle Dateien und Verzeichnisse entfernt, die bei der Installation der Software erstellt wurden.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Navigieren Sie mit dem folgenden Befehl zum Ordner "*bin*", in dem Arcserve Unified Data Protection Agent for Linux installiert ist:

   ```
   # cd /opt/CA/d2dserver/bin/
   ```

3. Führen Sie folgenden Befehl aus, um Arcserve UDP Agent (Linux) zu deinstallieren:

   ```
   # ./d2duninstall
   ```

   Eine Meldung wird angezeigt, nachdem die Deinstallation abgeschlossen wurde.

Arcserve UDP Agent (Linux) wurde vom Server deinstalliert.

Überprüfen der Deinstallation

Überprüfen Sie, dass Arcserve UDP Agent (Linux) vom Server entfernt wurde, wenn der Deinstallationsvorgang abgeschlossen ist.

Navigieren Sie zum folgenden Ordner, und überprüfen Sie, ob Arcserve UDP Agent (Linux) entfernt wurde:

```
/opt/CA/d2dserver
```

Sie haben die Deinstallation von Arcserve UDP Agent (Linux) überprüft. Arcserve UDP Agent (Linux) wurde vom Linux-Server entfernt.

So führen Sie ein Upgrade von Arcserve UDP Agent (Linux) aus

Führen Sie ein Upgrade von Arcserve UDP Agent (Linux) auf die nächste Version durch, um eine Reihe von Änderungen und Verbesserungen der Funktionen und Leistung von Arcserve UDP Agent (Linux) zu nutzen.

Folgendes Diagramm zeigt den Upgrade-Vorgang für Arcserve UDP Agent (Linux):

So aktualisieren Sie Arcserve Unified Data Protection Agent für Linux
Speicherverwaltung
Hinweise zur Aktualisierung
Aktualisieren von Arcserve Unified Data Protection Agent für Linux
Überprüfen der Aktualisierung

Gehen Sie wie folgt vor, um ein Upgrade für Arcserve UDP Agent (Linux) durchzuführen:

- Zu Aktualisierungen (siehe Seite 20)
- Durchführen eines Upgrades von Arcserve UDP Agent (Linux) (siehe Seite 21)
- Überprüfen des Upgrade (siehe Seite 23)

Zu Aktualisierungen

Beachten Sie die folgenden Punkte, bevor Sie mit dem Upgrade beginnen:

- Stellen Sie sicher, dass Sie Ihr Upgrade für einen Zeitpunkt planen, zu dem keine Sicherungsjobs ausgeführt werden.
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Durchführen eines Upgrades von Arcserve UDP Agent (Linux)

Führen Sie ein Upgrade von Arcserve UDP Agent (Linux) auf die nächste Version durch, um eine Reihe von Änderungen und Verbesserungen der Funktionen und Leistung von Arcserve UDP Agent (Linux) zu nutzen.

Wenn Sie das Upgrade installieren, versucht Arcserve UDP Agent (Linux), eine vorhandene Installation zu erkennen.

- Wenn Arcserve UDP Agent (Linux) eine vorhandene Installation erkennt, wird der Upgrade-Vorgang automatisch ausgeführt. Alle vorhandenen Konfigurationen (Konfigurationsdateien, Datenbank usw.) werden gespeichert und aktualisiert.
- Wenn Arcserve UDP Agent (Linux) keine vorhandene Installation erkennt, wird automatisch eine Neuinstallation ausgeführt.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Laden Sie das Arcserve UDP Agent (Linux)-Installationspaket (*.bin-Datei) und die Paketdatei mit dem Wiederherstellungshilfsprogramm in den Stammordner herunter.

   Wichtig! Wenn Sie die zwei Dateien des Installationspakets in einen lokalen Ordner herunterladen, dann darf der vollständige Pfad dieses lokalen Ordners keine Sonderzeichen (mit Ausnahme von Leerzeichen) enthalten, und der Pfad sollte nur folgende Zeichen umfassen: a-z, A-Z, 0-9, - und _.
3. Geben Sie dem Installationspaket Ausführungsberechtigungen.

4. Führen Sie einen der folgenden Schritte je nach Speicherort des Installationspakets und des Wiederherstellungs-Hilfsprogrammpakets aus:

   - Wenn das Installationspaket und das Wiederherstellungs-Hilfsprogrammpaket im gleichen Ordner sind, dann führen Sie folgenden Befehl aus, um die Installation zu beginnen:

     ```
     ./<linux_installation_file_name>.bin
     ```

     Hinweis: Wenn Sie das Paket mit dem Wiederherstellungshilfsprogramm umbenennen, dann muss der Paketname die Zeichen des Wiederherstellungshilfsprogramms enthalten, damit der Installationsbefehl das Paket mit dem Wiederherstellungshilfsprogramm automatisch findet und installiert. Wenn der Paketname die Zeichen des Wiederherstellungshilfsprogramms nicht enthält, müssen Sie den vollständigen Pfad des Pakets mit dem Wiederherstellungshilfsprogramm angeben.

     Das Installationspaket überprüft die unterstützte Plattform und zeigt eine Bestätigungsmeldung an.

     Wenn eine nicht unterstützte Plattform erkannt wird, tippen Sie "Y" und drücken Sie die Eingabetaste, um die Installation der nicht unterstützten Plattform zu bestätigen.

   - Wenn das Installationspaket und das Paket mit dem Wiederherstellungshilfsprogramm sich in verschiedenen Ordnern befinden, dann geben Sie den Pfad des Pakets mit dem Wiederherstellungshilfsprogramm im ersten Parameter an:

     ```
     ./<Linux_Installationsdateiname>.bin
     –-path=/<Pfad_des_Pakets_mit_dem_Wiederherstellungshilfsprogramm>
     ```

     Das Installationspaket überprüft die unterstützte Plattform und zeigt eine Bestätigungsmeldung an.

     Wenn eine nicht unterstützte Plattform erkannt wird, tippen Sie "Y" und drücken Sie die Eingabetaste, um die Installation der nicht unterstützten Plattform zu bestätigen.

   Das Installationspaket erkennt eine vorhandene Installation und zeigt eine Bestätigungsmeldung für das Upgrade an.

5. (Optional) Tippen Sie "Y" und drücken Sie die Eingabetaste, um Anwendungsabhängigkeiten zu bestätigen.

   Das Installationspaket überprüft die Anwendungsabhängigkeiten.

6. Geben Sie "J" ein, und drücken Sie die Eingabetaste, um die Installation zu bestätigen.

   Das Installationspaket zeigt die Informationen zur Lizenzierungsvereinbarung an.

7. Geben Sie "J" ein, und drücken Sie die Eingabetaste, um die Lizenzierungsvereinbarung zu akzeptieren.

   Der Arcserve UDP Agent (Linux)-Installationsprozess beginnt.

   Wenn die Installation des Pakets mit dem Wiederherstellungshilfsprogramm abgeschlossen ist, werden die Live-CD-Build-Informationen angezeigt.

   Die Live-CD wird am folgenden Speicherort erzeugt:

   `/opt/CA/d2dserver/packages`

   Hinweis: Live-CD ist erforderlich, um die IP-Adresse des Zielknotens abzurufen, wenn Sie eine Bare-Metal-Recovery (BMR) ausführen.

Das Arcserve UDP Agent (Linux)-Upgrade wurde erfolgreich durchgeführt.

Überprüfen des Upgrade

Stellen Sie nach dem Upgrade von Arcserve UDP Agent (Linux) auf die nächste Version sicher, dass das Upgrade abgeschlossen ist. Der Sicherungsserver speichert eine Sicherung der vorhandenen Konfigurationsdateien. Löschen Sie nach Abschluss der Überprüfung die Sicherungskopie der vorhandenen Konfigurationsdateien.

Gehen Sie wie folgt vor:

1. Öffnen Sie auf einem Windows-Computer einen Webbrowser.
2. Definiert die URL des Sicherungsservers.

   Beispiel: https://hostname:8014

   Die Anmeldeseite von Arcserve UDP Agent (Linux) wird geöffnet.
3. Geben Sie Ihre root-Anmeldeinformationen ein, und klicken Sie auf "Anmelden".

   Die Arcserve UDP Agent (Linux)-Benutzeroberfläche wird geöffnet.
4. Stellen Sie sicher, dass der Sicherungsserver ordnungsgemäß funktioniert.
5. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
6. Navigieren Sie zum Ordner "d2dserver.bak", und löschen Sie ihn.

   `/opt/CA/d2dserver.bak`

Arcserve UDP Agent (Linux) wurde erfolgreich aktualisiert und überprüft.

Kapitel 3: Benutzeroberfläche

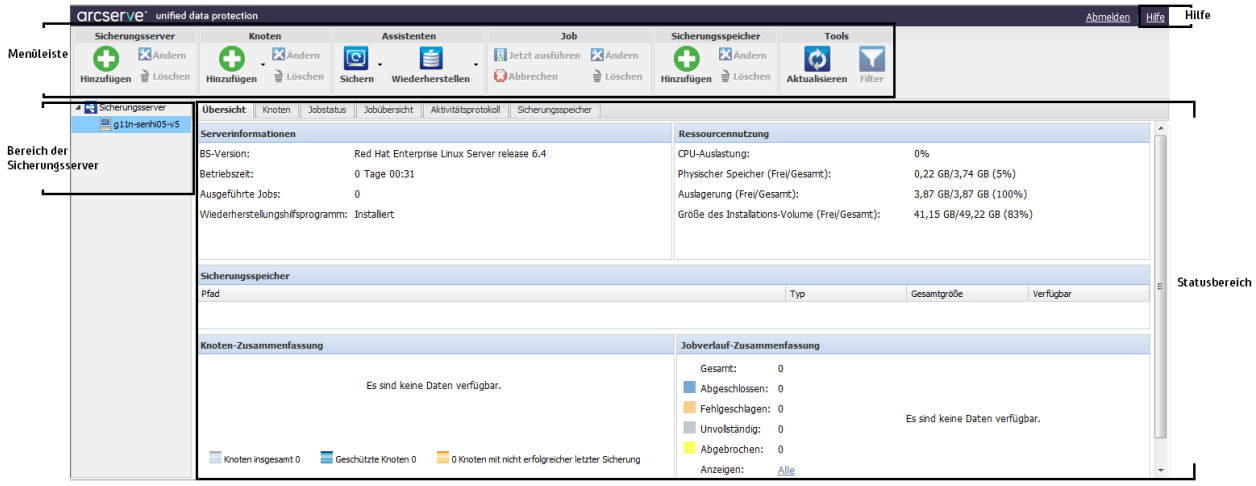
Dieses Kapitel enthält folgende Themen:

[So navigieren Sie in der Benutzeroberfläche von Arcserve UDP Agent (Linux)](#) (siehe Seite 25)

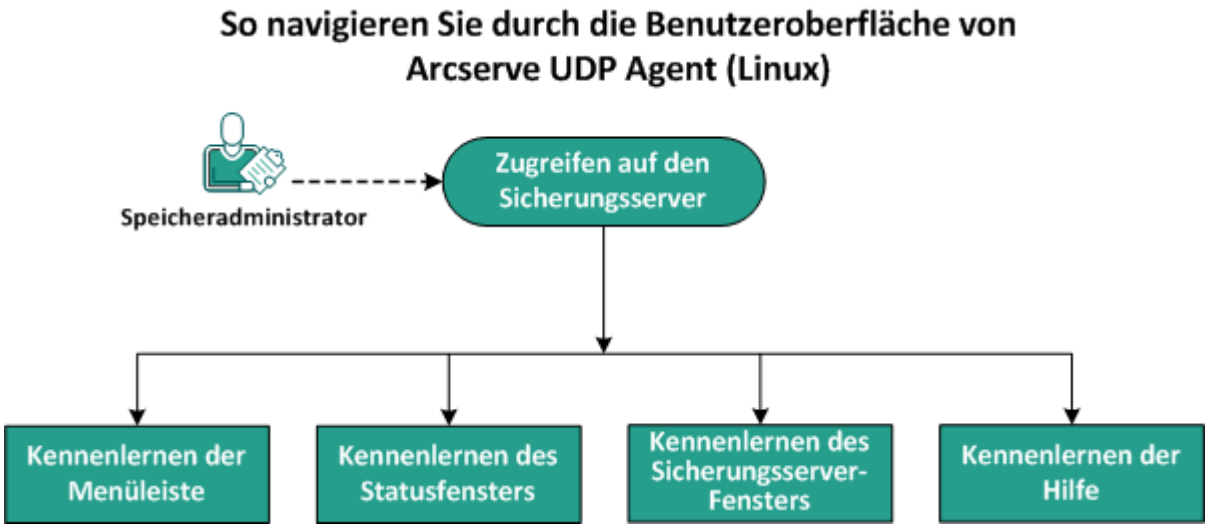
So navigieren Sie in der Benutzeroberfläche von Arcserve UDP Agent (Linux)

Bevor Sie Arcserve UDP Agent (Linux) verwenden, müssen Sie sich mit der Benutzeroberfläche vertraut machen. Über die Benutzeroberfläche können Sie Knoten, Sicherungsziele sowie Sicherungs- und Wiederherstellungsjobs verwalten und auf die Hilfethemen zugreifen.

Die Benutzeroberfläche der Startseite besteht aus vier Hauptbereichen: Menüleiste, Statusfenster, Sicherungsserver-Fenster und Hilfe.



Folgendes Diagramm zeigt den Vorgang an, um durch die Arcserve UDP Agent (Linux)-Schnittstelle zu navigieren:


So navigieren Sie durch die Benutzeroberfläche von Arcserve UDP Agent (Linux)
Speicheradministrator
Zugreifen auf den Sicherungsserver
Kennenlernen der Menüleiste
Kennenlernen des Statusfensters
Kennenlernen des Sicherungsserver-Fensters
Kennenlernen der Hilfe

Führen Sie diese Tasks aus, um die Benutzeroberfläche des Sicherungsservers zu verwenden:

- Zugreifen auf den Sicherungsserver (siehe Seite 27)
- Kennenlernen der Menüleiste (siehe Seite 27)
- Kennenlernen des Statusfensters (siehe Seite 30)
- Kennenlernen des Sicherungsserver-Fensters (siehe Seite 34)
- Kennenlernen der Hilfe (siehe Seite 35)

Zugreifen auf den Sicherungsserver

Als Storage Manager können Sie über die Web-Benutzeroberfläche auf den Sicherungsserver zugreifen. Melden Sie sich mit Root- oder Nicht-Root-Anmeldeinformationen an, um auf den Sicherungsserver zuzugreifen. Verwenden Sie die IP-Adresse, die Sie während der Installation von Arcserve UDP Agent (Linux) erhalten haben, um sich beim Server anzumelden. Wenn Sie den Hostnamen des Servers notiert haben, können Sie sich mit dem Hostnamen beim Server anmelden.

Hinweis: Weitere Informationen zur Angabe der Anmeldeberechtigung für Nicht-Root-Benutzer finden Sie unter Gewähren von Anmeldeberechtigungen für Nicht-Root-Benutzer.

Gehen Sie wie folgt vor:

1. Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse des Sicherungsservers ein.

   Hinweis: Standardmäßig folgt der Sicherungsserver https-Protokoll und verwendet den Port 8014.

2. Geben Sie die Anmeldeinformationen ein, und klicken Sie auf Anmelden.

   Die Benutzeroberfläche des Sicherungsserver wird geöffnet.

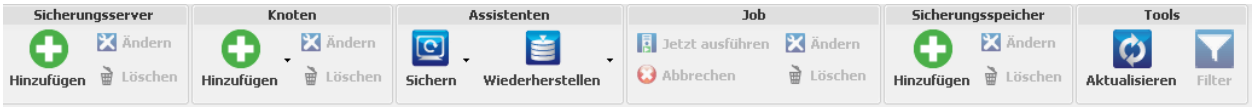
Auf den Sicherungsserver wurde erfolgreich zugegriffen.

Kennenlernen der Menüleiste

Über die Menüleiste können Sie die folgenden Aufgaben ausführen:

- Verwalten von Sicherungsservern
- Verwalten von Knoten
- Verwalten von Sicherungsjobs
- Verwalten von Wiederherstellungsjobs
- Verwalten von Sicherungsspeicherorten
- Filtern von Suchläufen
- Seiten aktualisieren

Folgende Abbildung zeigt die Menüleiste an:



Die Menüleiste umfasst die folgenden Optionen:

Sicherungsserver

Mit dieser Option können Sie Server, auf denen Arcserve UDP Agent (Linux) installiert ist, hinzufügen, ändern und löschen. Sie können Arcserve UDP Agent (Linux) auf mehreren Servern installieren und alle installierten Server über eine zentrale Benutzeroberfläche verwalten. Die Knoten, die vom ausgewählten Server verwaltet werden, werden im Statusfenster angezeigt. Alle hinzugefügten Server werden im Bereich "Sicherungsserver" angezeigt. Sie können den zentralen Server nicht ändern oder löschen. Ein zentraler Server ist der erste Server, der im Bereich "Sicherungsserver" angezeigt wird. Sie können andere Server aus dem Bereich "Sicherungsserver" ändern und löschen. Mit der Schaltfläche Ändern können Sie nur die Portnummer der Server aktualisieren.

Knoten

Ermöglicht Ihnen, zu sichernde Knoten hinzuzufügen, zu ändern und zu löschen. Knoten sind die Rechner, die Sie sichern möchten. Sie können mehrere zu sichernde Knoten hinzufügen. Sie können im Netzwerk vorhandene Knoten auch mithilfe eines Skripts ermitteln. Sie können für jeden Server höchstens 200 Knoten hinzufügen.

Wenn Sie einen Knoten löschen, löscht der Sicherungsserver alle Informationen zum Knoten aus der Datenbank, auch die Informationen zum Sicherungsjob. Der Sicherungsserver löscht auch die Treiber aus dem Knoten. Die komplette Löschung des Treibers kann etwas Zeit in Anspruch nehmen.

Assistenten

Ermöglicht Ihnen, den Sicherungsassistenten und den Wiederherstellungs-Assistenten zu starten, die Sie durch den Sicherungs- und Wiederherstellungsvorgang leiten.

- Der Sicherungsassistent enthält eine Drop-down-Liste mit drei verfügbaren Optionen:

  Sichern

  Verwenden Sie diese Option, wenn Sie noch keine zu sichernden Knoten hinzugefügt haben. Bei Auswahl dieser Option wird der Sicherungsassistent gestartet, und Sie können Knoten hinzufügen.

  Ausgewählte Knoten sichern

  Verwenden Sie diese Option, bevor Sie den Sicherungsassistenten starteten, wenn Sie bereits Knoten hinzugefügt haben. Wenn Sie auf Ausgewählte Knoten sichern klicken, ohne Knoten hinzuzufügen oder vorhandene Knoten auszuwählen, wird eine Fehlermeldung angezeigt. Um diesen Fehler zu vermeiden, wählen Sie den Knoten auf der Registerkarte "Knoten" aus, und wählen Sie dann "Ausgewählte Knoten sichern".

Ausgewählte Knoten zu einem vorhandenen Job hinzufügen

Verwenden Sie diese Option, wenn Sie einen vorhandenen Sicherungsjob haben und Sie die gleichen Sicherungseinstellungen auf neue Knoten anwenden möchten. Sie müssen den Sicherungsassistenten nicht konfigurieren.

- Der Wiederherstellungs-Assistent enthält eine Drop-down-Liste mit zwei verfügbaren Optionen:

  Bare-Metal-Recovery (BMR)

  Verwenden Sie diese Option zum Ausführen einer BMR. Sie können eine BMR anhand der IP-Adresse oder der MAC-Adresse des wiederherzustellenden Bare-Metal-Computers ausführen.

  Wiederherstellungsdatei

  Verwenden Sie diese Option, um eine Wiederherstellung auf Dateiebene auszuführen. Sie können bestimmte Dateien aus einem Wiederherstellungspunkt auswählen und diese Dateien wiederherstellen.

Job

Ermöglicht Ihnen die Verwaltung von Jobs, die Sie erstellen. Ein Job ist eine Instanz eines Sicherungs- oder Wiederherstellungsvorgangs. Nachdem Sie einen Sicherungsjob für einen Knoten erstellt haben, müssen Sie keinen weiteren Job erstellen, um das nächste Mal für denselben Knoten eine Sicherung auszuführen. Sie müssen jedoch immer einen Wiederherstellungsjob erstellen, wenn Sie eine BMR ausführen möchten.

Sicherungsspeicher

Ermöglicht Ihnen, die Sicherungsspeicherorte hinzuzufügen und zu verwalten. Der Sicherungsspeicherort kann eine Network File System (NFS)-Freigabe oder eine Common Internet File System (CIFS)-Freigabe oder eine lokale Freigabe sein. Lokal ist ein lokaler Pfad im Sicherungsserver.

Wenn Sie einen Sicherungsspeicherort hinzufügen, müssen Sie Ihre Anmeldeinformationen für den ausgewählten Sicherungsspeicherort angeben. Sie können nur den Benutzernamen und das Kennwort der CIFS-Freigabe ändern. Sie können keine Details der NFS-Freigabe ändern. Wählen Sie das Kontrollkästchen Skript ausführen bei freiem Speicherplatz unter aus, um das Skript *backup_storage_alert.sh* auszuführen, wenn der freie Speicherplatz unter dem angegebenen Wert liegt. Dieser Wert kann ein Prozentsatz des gesamten Speicherplatzes am Sicherungsziel oder der minimale Speicherplatz (in MB) am Sicherungsziel sein. Das Skript "backup_storage_alert.sh" kann konfiguriert werden, um einen Alert zu senden, wenn der verfügbare freie Speicherplatz weniger ist als der angegebene Wert.

Hinweis: Weitere Informationen über das Konfigurieren des Skripts "backup_storage_alert.sh" finden Sie unter *So integrieren und automatisieren Sie Arcserve UDP Agent (Linux) in einer bestehenden IT-Umgebung*.

Nachdem Sie einen Sicherungsspeicherort hinzugefügt haben, können Sie die entsprechende gesamte Dateigröße und den freien Platz im Statusfenster anzeigen. Wählen Sie einen Sicherungsspeicherort aus, um die Wiederherstellungssätze und Wiederherstellungspunkte und den verwendeten Speicherplatz für jeden Knoten anzuzeigen, die in diesem Sicherungsspeicherort sichergestellt werden. Die hinzugefügten Speicherziele werden auch auf der Seite "Sicherungsziel" des Sicherungsassistenten und auf der Seite "Wiederherstellungspunkte" des Wiederherstellungs-Assistenten angezeigt.

Tools

Das Menü "Tools" umfasst die Schaltflächen "Aktualisieren" und "Filtern".

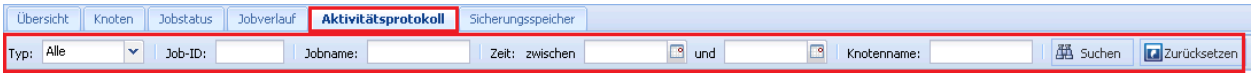
Aktualisieren

Ermöglicht es Ihnen, den ausgewählten Anzeigebereich im Statusfenster (einschließlich Aktivitätsprotokoll) zu aktualisieren, um die aktuellen Sicherungs- oder Wiederherstellungs-Statusmeldungen anzuzeigen.

Filter

Ermöglicht es Ihnen, Informationen zu filtern, die basierend auf Ihrer Eingabe im Statusbereich angezeigt werden. Die Schaltfläche "Filtern" funktioniert wie ein Schalter, sodass Sie Filter mithilfe der gleichen Schaltfläche aktivieren und deaktivieren können. Wenn Sie Filter aktivieren, werden die Suchfelder im Statusfenster angezeigt. Wenn Sie Filter deaktivieren, werden die Suchfelder aus dem Statusfenster entfernt.

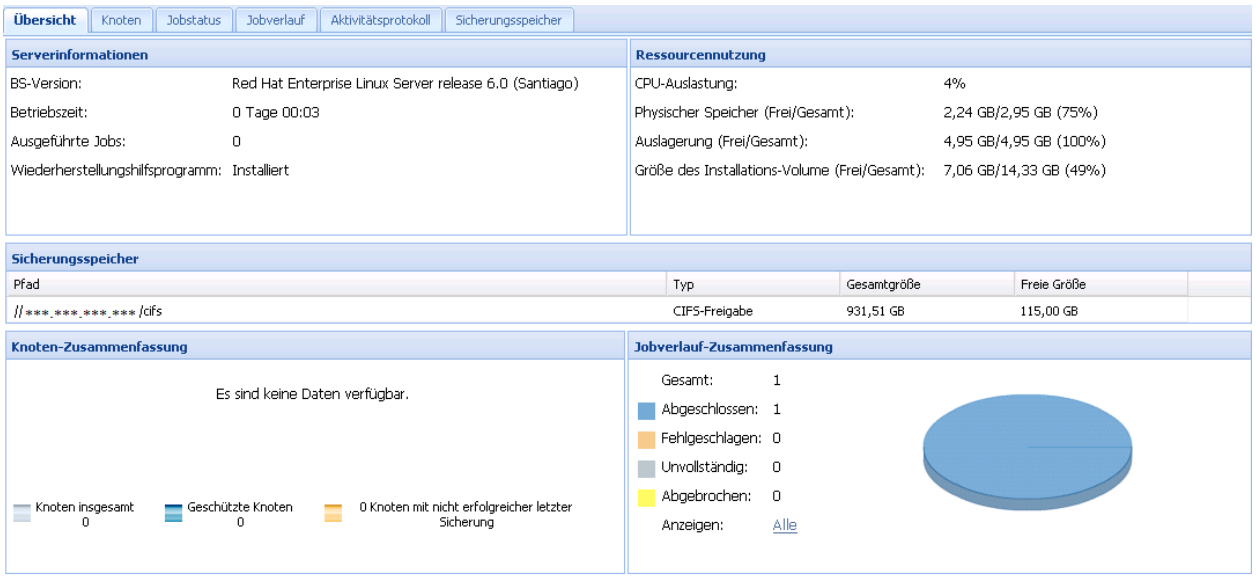
Folgende Abbildung zeigt die Filter an, die auf das Aktivitätsprotokoll angewendet werden:



Kennenlernen des Statusfensters

Das Statusfenster ist der Bereich, in dem alle Informationen der Benutzeroberfläche angezeigt werden. Das Statusfenster umfasst sechs Registerkarten, auf denen die jeweils relevanten Informationen angezeigt werden.

Folgende Abbildung zeigt den Statusbereich an:



Das Statusfenster verfügt über die folgenden Registerkarten:

Übersicht

Gibt eine Übersicht über die folgenden Elemente:

Serverinformationen

Zeigt die Version des Betriebssystems, die seit dem Serverstart verstrichene Zeit und die Lizenzierungsinformation für Arcserve UDP Agent (Linux) an. Es wird auch angezeigt, ob das Wiederherstellungs-Hilfsprogramm auf diesem Server installiert ist.

Ressourcennutzung

Zeigt die Nutzung der CPU, den gesamten und verfügbaren physischen Speicher sowie die Swap-Größe an. Darüber hinaus wird die Größe des Installationsvolumes angezeigt.

Sicherungsspeicher

Zeigt alle Sicherungssitzungs-Speicherorte an, die Sie hinzugefügt haben, sowie den verfügbaren Speicherplatz an jedem Speicherort. Anhand dieser Informationen können Sie den nächsten Sicherungsspeicherort je nach dem verfügbarem Speicherplatz planen.

Knoten-Zusammenfassung

Zeigt eine grafische Darstellung der Knoten an, die geschützt sind, sowie der Knoten, die zuletzt erfolglos gesichert wurden. "Knoten-Zusammenfassung" schließt die folgenden Kategorien ein:

"Knoten insgesamt" zeigt die Anzahl der in Arcserve UDP Agent (Linux) vorhandenen Knoten an, ungeachtet des Sicherungsstatus.

"Geschützte Knoten" zeigt die Anzahl der Knoten an, für die die letzte Sicherung erfolgreich durchgeführt wurde, und die im Falle einer notwendigen Wiederherstellung als geschützt betrachtet werden.

"Knoten mit nicht erfolgreicher letzter Sicherung" gibt die Anzahl der Knoten an, deren letzte Sicherung nicht erfolgreich war (fehlgeschlagen, abgebrochen, unvollständig). Je nach Ursache der erfolglosen Sicherung können einige dieser Knoten ungeschützt sein, falls eine Wiederherstellung notwendig ist.

Jobverlauf-Zusammenfassung

Zeigt ein Kreisdiagramm an, das den Verlauf aller Jobs zusammenfasst. Die Übersicht schließt die gerade ausgeführten Jobs nicht ein.

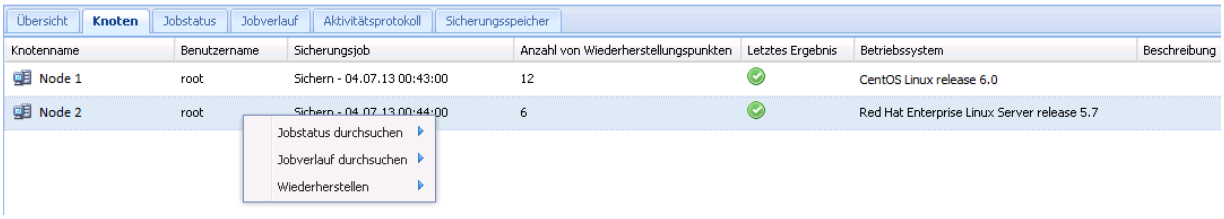
Die folgenden Felder sind nicht selbsterklärend:

"Unvollständig" zeigt die Anzahl der Jobs an, die erfolgreich mit kleineren Änderungen ausgeführt wurden. Wenn Sie zum Beispiel Wiederherstellungen von Dateien von "Red Hat 6" auf "Red Hat 5" durchführen, dann werden die Dateien erfolgreich wiederhergestellt, jedoch fehlen einige Attribute in den wiederhergestellten Dateien.

"Andere" zeigt die Anzahl der Jobs an, die Sie abgebrochen haben.

Knoten

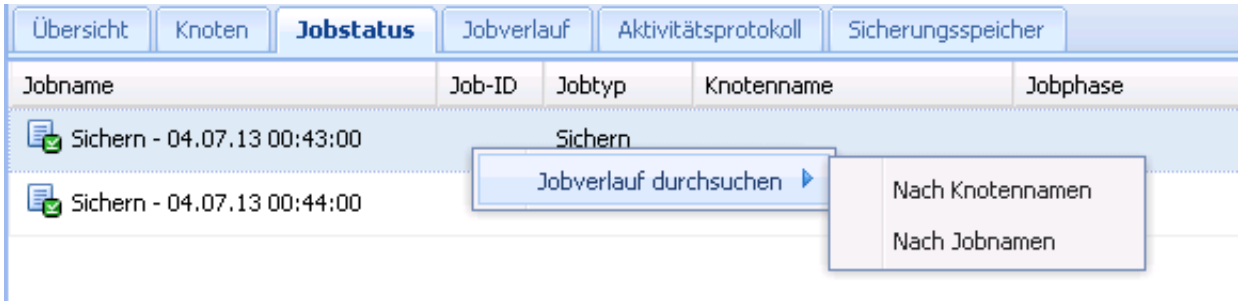
Zeigt alle Knoten an, die Sie dem Sicherungsserver hinzugefügt haben. Sie können Filter auf die Registerkarte "Knoten" anwenden, um nach den gewünschten Knoten zu suchen. Die Registerkarte Knoten umfasst auch ein Kontextmenü. Im Kontextmenü können Sie den Jobstatus oder den Jobverlauf für den ausgewählten Knoten suchen. Mit dem Kontextmenü können Sie auf Daten wiederherstellen. Sie können den Jobverlauf oder den Jobstatus filtern, indem Sie entweder den Jobnamen oder den Knotennamen verwenden. Wenn Sie den Jobverlauf für den ausgewählten Knoten suchen, dann wird die Registerkarte Jobverlauf mit dem Suchfilter geöffnet, der auf die Registerkarte angewendet wurde. Wenn Sie den Jobstatus suchen, dann wird die Registerkarte Jobstatus in gleicher Weise mit dem Suchfilter geöffnet, der auf die Registerkarte angewendet wurde. Mit der Wiederherstellungsoption können Sie BMR oder eine Wiederherstellung auf Dateiebene ausführen. Der Wiederherstellungs-Assistent wird geöffnet, und es werden alle Wiederherstellungspunkte des ausgewählten Knotens angezeigt.



Jobstatus

Zeigt die Liste der erstellten Sicherungs- und Wiederherstellungsjobs an, einschließlich des Status jedes Jobs. Verwenden Sie diese Registerkarte, um einen Sicherungs- oder Wiederherstellungsjob auszuführen und einen Sicherungsjob zu wiederholen. Sie können den Fortschritt der Sicherungs- oder Wiederherstellungsjobs sehen, die Sie ausführen. Sie können Filter auf die Registerkarte "Jobstatus" anwenden, um nach den gewünschten Jobs zu suchen. Die Registerkarte Jobstatus umfasst auch ein Kontextmenü. Im Kontextmenü können Sie im Jobverlauf nach dem ausgewählten Job suchen. Sie können den Jobverlauf filtern, indem Sie entweder den Jobnamen oder den Knotennamen verwenden. Wenn Sie im Jobverlauf den ausgewählten Job suchen, dann wird die Registerkarte "Jobverlauf" geöffnet, und der Suchfilter wird auf die Registerkarte angewendet.

Folgende Abbildung zeigt das Kontextmenü in der Registerkarte Jobstatus an:



Jobübersicht

Zeigt die Liste von Sicherungs- und Wiederherstellungsjobs an, die früher ausgeführt wurden. Sie können Filter auf die Registerkarte "Jobverlauf" anwenden, um nach dem gewünschten Jobverlauf zu suchen. Wenn Sie einen Job auswählen, wird der Status dieses Jobs unten auf der Seite angezeigt.

Aktivitätsprotokoll

Zeigt eine Liste von Verarbeitungsmeldungen und Statusmeldungen für Sicherungs- und Wiederherstellungsjobs an. Aktualisieren Sie das "Aktivitätsprotokoll", um die neuesten Meldungen für die letzten Sicherungs- und Wiederherstellungsjobs abzurufen. Sie können Filter auf die Registerkarte "Aktivitätsprotokoll" anwenden, um nach erforderlichen Aktivitätsprotokollen zu suchen.

Sicherungsspeicher

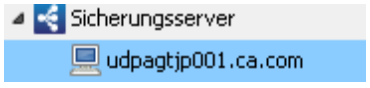
Zeigt das Sicherungsziel an, das Sie in der Menüleiste hinzugefügt haben. Sie können den freien Speicherplatz anzeigen und Ihr Sicherungsziel verwalten. Diese Option ist hilfreich, wenn Sie den verfügbaren Speicherplatz an einem bestimmten Sicherungsziel ermitteln möchten, um Ihre Sicherung zu planen. Wenn Sie ein Speicherziel hinzufügen, wird dieses Ziel im Sicherungsassistenten angezeigt.

Kennenlernen des Sicherungsserver-Fensters

Im Fenster "Sicherungsserver" wird eine Liste der Sicherungsserver angezeigt, die vom aktuellen Server verwaltet werden. Sie können Server in der Menüleiste hinzufügen und können alle Server über eine Benutzeroberfläche verwalten. Wenn Sie mehrere Server hinzugefügt haben, zeigt das Statusfenster den Status des ausgewählten Servers an. Jeder Server kann mindestens 200 Client-Knoten verwalten.

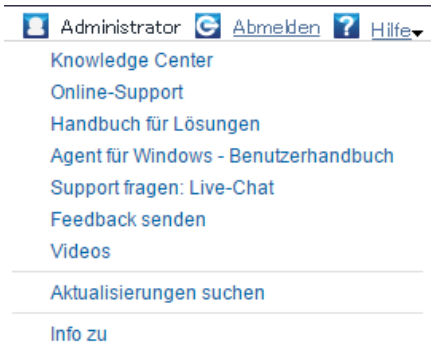
Normalerweise handelt es sich beim ersten Server, der im Bereich "Sicherungsserver" angezeigt wird, um den zentralen Sicherungsserver, und bei den weiteren Servern um Mitgliedsserver. Wenn Sie mehrere Server über einen zentralen Server verwalten, stellen Sie sicher, dass die Version des zentralen Servers und der Mitgliedsserver identisch sind.

Folgende Abbildung zeigt den Bereich "Sicherungsserver":



Kennenlernen der Hilfe

Mit dem Dialogfeld "Hilfe" können Sie auf Hilfethemen von Arcserve UDP Agent (Linux) zugreifen. Über die Drop-down-Liste Hilfe können Sie folgende Aufgaben durchführen:



Folgende Optionen sind in der Drop-down-Liste Hilfe verfügbar:

Knowledge Center

Ermöglicht es Ihnen, auf das Bookshelf zuzugreifen.

Hilfe (HTML)

Ermöglicht es Ihnen, auf die HTML-Version des Arcserve UDP Agent (Linux)-Benutzerhandbuchs zuzugreifen.

Benutzerhandbuch

Ermöglicht es Ihnen, auf die PDF-Version des Arcserve UDP Agent (Linux)-Benutzerhandbuchs zuzugreifen.

Zugriff auf Support und Community

Ermöglicht es Ihnen, auf die Arcserve UDP Agent (Linux)-Support-Seite und auf die ARCserve-Community-Seiten zuzugreifen. Sie können folgende Aufgaben über "Zugriff auf Support und Community" ausführen:

- Produkteinzelheiten anzeigen
- Auf die offizielle ARCserve-Website zugreifen
- Feedback für die Entwickler bereitstellen
- Tipps und Kommentare von ARCserve-Fachleuten lesen

- Mit einem Support-Manager chatten
- RSS-Feeds abonnieren

Lizenz verwalten

Ermöglicht es Ihnen, auf das Dialogfeld Lizenzverwaltung zuzugreifen und Ihre gesamten Lizenzen über eine zentrale Schnittstelle zu verwalten.

Info zu

Ermöglicht es Ihnen, die Produktinformationen anzuzeigen (Versionsnummer und Build-Nummer) und auf die Versionshinweise von Arcserve UDP zugreifen.

Kapitel 4: Verwenden von Arcserve UDP Agent (Linux)

Dieses Kapitel enthält folgende Themen:

So verwalten Sie die Lizenzen (siehe Seite 37)
So verwalten Sie Jobs (siehe Seite 41)
So sichern Sie Linux-Knoten (siehe Seite 44)
So ändern Sie einen Sicherungsjob und führen ihn erneut aus (siehe Seite 76)
So führen Sie eine Wiederherstellung der Dateiebene unter Linux-Knoten aus (siehe Seite 80)
So erstellen Sie eine startfähige Live-CD (siehe Seite 98)
So erstellen Sie eine CentOS-basierte Live-CD (siehe Seite 102)
So führen Sie eine Bare-Metal-Recovery (BMR) für Linux-Rechner aus (siehe Seite 106)
So stellen Sie einen virtuellen Rechner automatisch wieder her (siehe Seite 130)
So integrieren und automatisieren Sie Arcserve Unified Data Protection Agent for Linux in einer bestehenden IT-Umgebung (siehe Seite 142)
So verwalten Sie die Einstellungen des Sicherungsservers (siehe Seite 177)
So verwalten Sie einen Linux-Sicherungsserver über die Befehlszeile (siehe Seite 185)
So verwalten Sie Nicht-Root-Benutzer (siehe Seite 198)
So stellen Sie Volumes auf einem Zielknoten wieder her (siehe Seite 202)
So stellen Sie eine Oracle-Datenbank mithilfe von Arcserve UDP Agent (Linux) wieder her (siehe Seite 211)

So verwalten Sie die Lizenzen

Sie müssen Arcserve UDP Agent (Linux) lizensieren, um autorisierten und unterbrechungsfreien Zugriff auf die dazugehörigen Komponenten zu erhalten. Wenn Sie Arcserve Unified Data Protection Agent for Linux per Remote-Zugriff bereitstellen möchten, müssen Sie zusätzlich die entsprechenden Remote-Standorte lizenzieren, um die Vorteile von Arcserve UDP Agent (Linux) voll auszuschöpfen.

Arcserve UDP Agent (Linux) wird als Testversion für einen Zeitraum von 30 Tagen ab Beginn der Verwendung funktionieren. Wenden Sie dann einen entsprechenden Lizenzschlüssel an, um das Produkt weiterhin zu verwenden. Mit Arcserve UDP Agent (Linux) können Sie die Lizenzen für alle Ihre Linux-Sicherungsserver über eine zentrale Schnittstelle verwalten.

Folgendes Diagramm zeigt den Prozess an, um Lizenzen zu verwalten:

Schließen Sie folgende Aufgaben ab, um die Lizenzen zu verwalten:

- Zugriff auf den Lizenzmanager (siehe Seite 38)
- Funktionsweise des Dialogfeldes "Lizenzverwaltung" (siehe Seite 39)
- Verwalten der Lizenzen (siehe Seite 40)

Zugriff auf den Lizenzmanager

Sie müssen auf das Dialogfeld "Lizenzverwaltung" von der Arcserve UDP Agent (Linux)-Webbenutzeroberfläche zugreifen, um alle Ihre Lizenzen zu verwalten.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Arcserve UDP Agent (Linux)-Webbenutzeroberfläche an.
2. Klicken Sie auf der Startseite auf Hilfe, Lizenz verwalten.

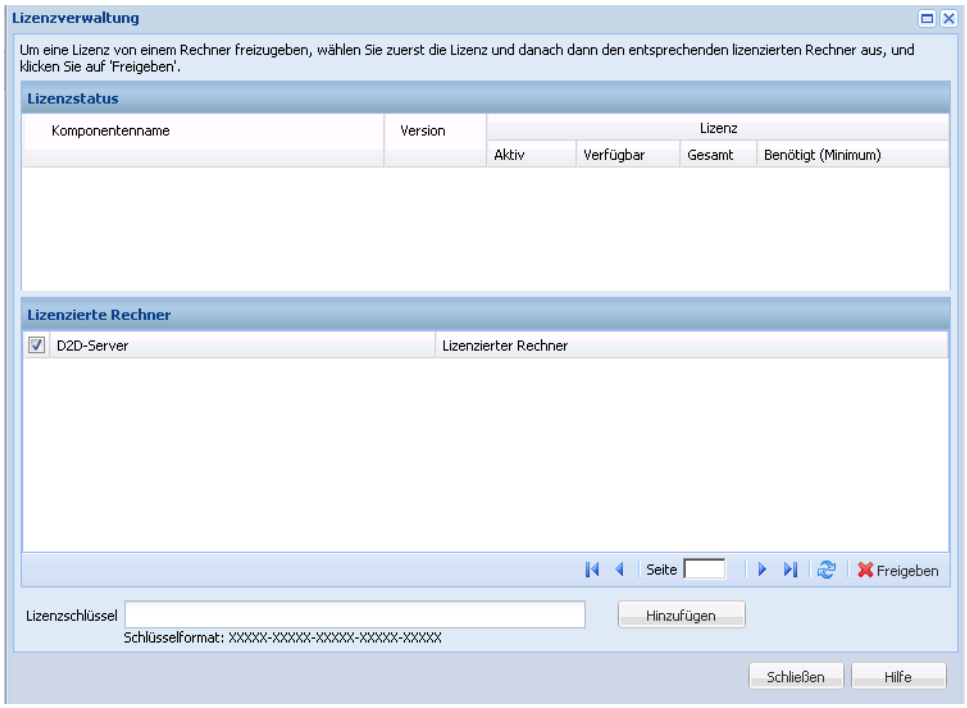
   Das Dialogfeld "Lizenzverwaltung" wird geöffnet.

Es erfolgt der Zugriff auf den Lizenzmanager.

Funktionsweise des Dialogfeldes "Lizenzverwaltung"

Mit dem Dialogfeld "Lizenzverwaltung" können Sie alle Ihre Lizenzen für Arcserve UDP Agent (Linux) verwalten. Sie können die Lizenzen für mehrere Linux-Sicherungsserver von einer einzelnen Schnittstelle verwalten.

Folgende Abbildung zeigt das Dialogfeld Lizenzverwaltung an:



Das Dialogfeld Lizenzverwaltung ist in zwei Abschnitte aufgeteilt: Lizenzstatus und Lizenzierte Rechner.

Lizenzstatus

Komponentenname

Identifiziert den Namen der Lizenz.

Version

Identifiziert die Versionsnummer der Lizenz.

Active (Aktiv)

Identifiziert die Anzahl der Lizenzen, die derzeit verwendet werden, um die Knoten zu sichern.

Verfügbar

Identifiziert die Anzahl der Lizenzen, die noch im Lizenzbestand verfügbar sind und die für die Sicherung von Linux-Rechnern verwendet werden können.

Gesamt

Identifiziert die gesamte Anzahl der Lizenzen, die abgerufen wurden, um den Rechner zu sichern. "Gesamt" ist die Summe der aktiven und verfügbaren Lizenzen.

Lizenzierte Rechner

Sicherungsserver

Identifiziert den Linux-Server, auf dem Arcserve UDP Agent (Linux) installiert ist.

Lizenzierte Rechner

Identifiziert die Linux-Rechner, für die Sie eine Lizenz angewendet haben, um diese Rechner zu schützen.

Verwalten der Lizenzen

Sie können Lizenzen vom Dialogfeld Lizenzverwaltung hinzufügen und freigeben. Die hinzugefügte Lizenz wird im Dialogfeld Lizenzverwaltung angezeigt. Wenn Sie keine Rechner mehr sichern möchten, können Sie die Lizenz von diesem Rechner freigeben.

Gehen Sie wie folgt vor:

- Um eine Lizenz hinzuzufügen, gehen Sie folgendermaßen vor:
  a. Überprüfen Sie den Lizenzschlüssel auf Ihrem Datenträger oder auf Ihrem Lizenzzertifikat.
  b. Geben Sie den Lizenzschlüssel in das Feld Lizenzschlüssel ein, und klicken Sie auf Hinzufügen.
  c. Schließen und öffnen Sie das Dialogfeld Lizenzverwaltung.

  Die Lizenz wird hinzugefügt und im Bereich Lizenzstatus aufgelistet.

- Um eine Lizenz freizugeben, gehen Sie folgendermaßen vor:
  a. Wählen Sie die Lizenz aus dem Bereich Lizenzstatus aus.
  b. Wählen Sie den Sicherungsserver aus "Lizenzierte Rechner" aus, und klicken Sie auf "Freigeben".
  c. Schließen und öffnen Sie das Dialogfeld Lizenzverwaltung.

     Die Lizenz wird vom Rechner freigegeben.

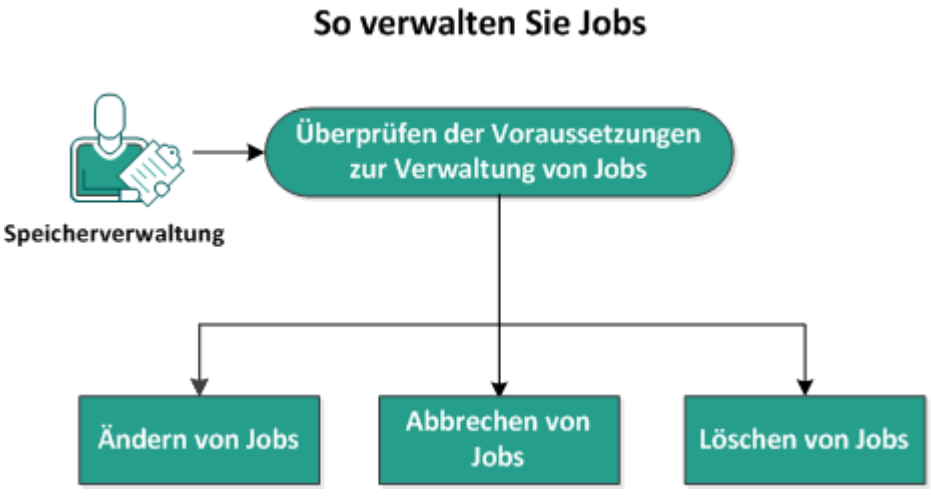
Die Lizenzen sind erfolgreich verwaltet.

So verwalten Sie Jobs

Nachdem Sie eine Sicherung oder einen Wiederherstellungsjob erstellt haben, können Sie Ihre gesamten Jobs im über das Menü Job verwalten. Das Verwalten von Jobs umfasst folgende Aufgaben:

- Ändern von Jobs
- Abbrechen von Jobs
- Löschen von Jobs

Folgendes Diagramm zeigt den Vorgang für die Verwaltung von Jobs:



Führen Sie diese Aufgaben aus, um Ihre Jobs zu verwalten:

- Überprüfen der Voraussetzungen (siehe Seite 42)
- Ändern von Jobs (siehe Seite 42)
- Abbrechen von Jobs (siehe Seite 42)
- Löschen von Jobs (siehe Seite 43)

Überprüfen der Voraussetzungen zur Verwaltung von Jobs

Beachten Sie folgende Voraussetzungen, bevor Sie Ihre Jobs verwalten:

- Sie haben einen gültigen vorhandenen Job, der verwaltet werden soll
- Sie haben die entsprechenden Berechtigungen, um Jobs zu verwalten.
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Ändern von Jobs

Sie können einen vorhandenen Job öffnen, und Sie können die Einstellungen für den Job über die Webschnittstelle ändern. Wenn Sie zum Beispiel das Sicherungsziel für einen bereits geschützten Rechner ändern möchten, müssen Sie keinen neuen Job erstellen. Sie können den vorhandenen Job öffnen, der den Rechner schützt, und nur den Abschnitt des Sicherungsziels ändern. Alle anderen Einstellungen bleiben unverändert mit Ausnahme der Sicherungszieleinstellungen.

Gehen Sie wie folgt vor:

1. Wählen Sie einen Job aus der Registerkarte Jobstatus aus.
2. Klicken Sie im Menü Job auf Ändern.

   Der Assistent für den ausgewählten Job wird geöffnet.
3. Ändern Sie Ihre Einstellungen im Assistenten.
4. Klicken Sie auf der Seite Zusammenfassung des Assistenten auf Übergeben.

   Der Job wird übergeben, und je nach Einstellungen wird der Job ausgeführt.

Der Job wurde erfolgreich geändert.

Abbrechen von Jobs

Sie können einen ausgeführten Job über die Webschnittstelle von Arcserve UDP Agent (Linux) abbrechen.

Gehen Sie wie folgt vor:

1. Wählen Sie einen Job aus der Registerkarte Jobstatus aus.
2. Klicken Sie im Menü Job auf Abbrechen.

   Das Dialogfeld Job abbrechen wird angezeigt.

3. Aktivieren Sie eine der folgenden Optionen aus der Drop-down-Liste Job abbrechen für:

   Ausgewählten Knoten

   Gibt an, dass der Job nur für den ausgewählten Knoten abgebrochen wird.

   Alle vom ausgewählten Job geschützten Knoten

   Gibt an, dass der Job für alle Knoten abgebrochen wird, die vom ausgewählten Job geschützt werden.

4. Klicken Sie auf "OK".

   Der Job wird abgebrochen.

Löschen von Jobs

Sie können einen Job löschen, wenn Sie keinen Rechner mehr schützen oder wiederherstellen möchten. Sie können auch einen Job löschen, der eine Gruppe von Knoten schützt. Wenn Sie einen Job löschen, dann sind die zuvor gesicherten Wiederherstellungspunkte weiterhin im angegebenen Sicherungsziel verfügbar. Sie können diese Wiederherstellungspunkte verwenden, um Ihre Daten wiederherzustellen.

Für einen ausgeführten Job ist die Option "Löschen" inaktiv. Sie müssen den ausgeführten Job abbrechen und anschließend den Job löschen.

Gehen Sie wie folgt vor:

1. Wählen Sie einen Job aus der Registerkarte Jobstatus aus.
2. Klicken Sie im Menü Job auf Löschen.

   Das Dialogfeld Job löschen wird angezeigt.

3. Aktivieren Sie eine der folgenden Optionen aus der Drop-down-Liste Job löschen für:

   Ausgewählten Knoten

   Gibt an, dass der Job nur für den ausgewählten Knoten gelöscht wird.

   Alle vom ausgewählten Job geschützten Knoten

   Gibt an, dass der Job für alle Knoten gelöscht wird, die vom ausgewählten Job geschützt werden.

4. Klicken Sie auf "OK".

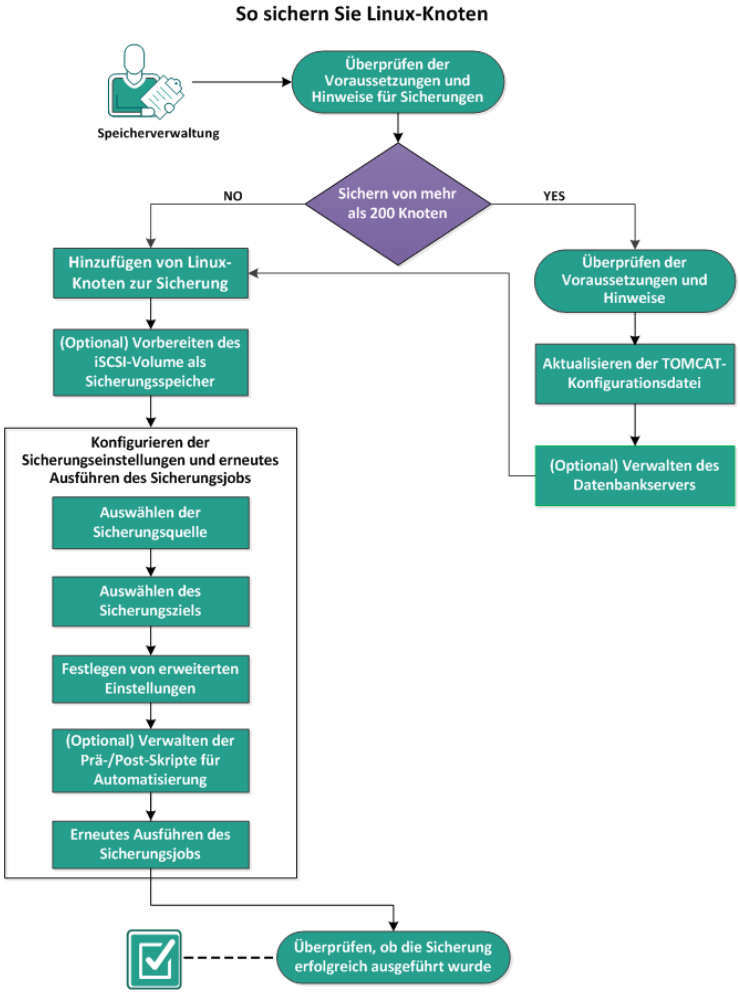
   Der Job wird gelöscht.

So sichern Sie Linux-Knoten

Mit Arcserve UDP Agent (Linux) können Sie Linux-Knoten und die darin gespeicherten Daten sichern. Sie können auch den Sicherungsserver selbst wie andere Linux-Knoten sichern. Der Sicherungsserver kann maximal 200 Knoten sichern.

Wenn Arcserve UDP Agent (Linux) eine Datensicherung ausführt, werden auch Informationen zum Betriebssystem, den installierten Anwendungen, Treibern usw. des Produktionsknotens einbezogen. Daher können Sie beim Wiederherstellen der gesicherten Daten eine BMR ausführen, oder Sie können einzelne Dateien wiederherstellen, die Sie benötigen.

Folgendes Diagramm zeigt, wie Linux-Knoten gesichert werden:


So sichern Sie Linux-Knoten
Speicherverwaltung
Überprüfen der Voraussetzungen und Hinweise für Sicherungen
Sichern von mehr als 200 Knoten
NO
YES
Hinzufügen von Linux-Knoten zur Sicherung
(Optional) Vorbereiten des iSCSI-Volume als Sicherungsspeicher
Konfigurieren der Sicherungseinstellungen und erneutes Ausführen des Sicherungsjobs
Auswählen der Sicherungsquelle
Auswählen des Sicherungsziels
Festlegen von erweiterten Einstellungen
(Optional) Verwalten der Prä-/Post-Skripte für Automatisierung
Erneutes Ausführen des Sicherungsjobs
Überprüfen der Voraussetzungen und Hinweise
Aktualisieren der TOMCAT-Konfigurationsdatei
(Optional) Verwalten des Datenbankservers
Überprüfen, ob die Sicherung erfolgreich ausgeführt wurde

Gehen Sie wie folgt vor, um einen Linux-Knoten zu sichern:

- Überprüfen der Voraussetzungen und Hinweise für Sicherungen (siehe Seite 45)
- Sichern von mehr als 200 Knoten (siehe Seite 47)
  - Überprüfen der Voraussetzungen und Hinweise (siehe Seite 48)
  - Aktualisieren der TOMCAT-Konfigurationsdatei (siehe Seite 49)
  - Verwalten des Datenbankservers
- Hinzufügen von Linux-Knoten zur Sicherung (siehe Seite 50)
- (Optional) Vorbereiten des iSCSI-Volume als Sicherungsspeicher (siehe Seite 53)
- Konfigurieren der Sicherungseinstellungen und erneutes Ausführen des Sicherungsjobs (siehe Seite 54)
  - Auswählen der Sicherungsquelle (siehe Seite 55)
  - Auswählen des Sicherungsziels (siehe Seite 58)
  - Festlegen von erweiterten Einstellungen (siehe Seite 62)
    - (Optional) Verwalten der Prä-/Post-Skripte für Automatisierung (siehe Seite 72)
  - Erneutes Ausführen des Sicherungsjobs (siehe Seite 75)
- Überprüfen, ob die Sicherung erfolgreich ausgeführt wurde (siehe Seite 76)

Überprüfen der Voraussetzungen und Hinweise für Sicherungen

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie eine Sicherung ausführen:

- Die Voraussetzungen für die unterstützte Hardware und Software für den Sicherungsknoten sind erfüllt.

  Hinweis: Weitere Informationen zu den Voraussetzungen für unterstützte Hardware und Software finden Sie in den *Versionshinweisen*.

- Sie verwenden ein gültiges Ziel zum Speichern der gesicherten Daten.
- Sie verfügen über die Benutzernamen und Kennwörter der Knoten, die Sie sichern möchten.
- Der Ordner */tmp* im Sicherungsknoten hat mindestens 300 MB Speicherplatz. Der Ordner */tmp* wird verwendet, um die Kumulierung von inkrementellen Blöcken zu verarbeiten.
- Perl und sshd (SSH-Daemon) sind auf den Knoten installiert, die Sie sichern möchten.
- "mount.nfs" ist auf den Knoten installiert, die Sie sichern möchten.

- "mount.cifs" ist auf den Knoten installiert, die Sie sichern möchten.
- Der Sicherungsknoten kann auf Ihr Sicherungsziel zugreifen, und Sie verfügen über Schreibberechtigungen.
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Um einen Sicherungsjob erneut auszuführen, stellen Sie sicher, dass Sie den Knoten bereits gesichert haben, und dass Sie über einen gültigen Sicherungsjob verfügen.

Überprüfen Sie folgende Sicherungshinweise:

- Um die Verwaltung Ihrer Wiederherstellungspunkte zu optimieren, sollten Sie folgende Empfehlungen beachten, wenn Sie die Häufigkeit Ihrer Sicherungen planen:
  - Für Systeme, die durch Zuwachssicherungen, die alle 15 Minuten ausgeführt werden, geschützt sind, sollten Sie eine wöchentliche vollständige Sicherung planen (um Ihr Basis-Image zu aktualisieren).
  - Für Systeme, die durch stündliche Zuwachssicherungen geschützt sind, sollten Sie eine monatliche vollständige Sicherung planen (um Ihr Basis-Image zu aktualisieren).

  Hinweis: Wenn der verwendete Speicherplatz für das Speichern Ihrer Sicherungs-Images ein Problem darstellt, dann sollten Sie in Erwägung ziehen, vollständige Sicherungen weniger häufig zu planen, um weniger Speicherplatz zu nutzen.

Von Arcserve UDP Agent (Linux) unterstützter Datenträger

Verschiedene Datenträgertypen werden für die Arcserve UDP Agent (Linux)-Sicherungsquelle und Sicherungsdatenträger unterstützt. Die folgende Matrix listet die Datenträgertypen auf, die für jede Funktion unterstützt werden.

Sicherung und BMR-Support		
Datenträgertyp (Volume)	**Als Sicherungsquelle**	**Als Sicherungsziel**
Geladenes Volume (Herkömmliche Datenträgerpartition und LVM ***2**)	Ja	Ja
RAW-Volume (Nicht formatiert)	Nein	Nein
Auslagerung	Nein	N/A
GPT-Datenträger:		

Sicherung und BMR-Support		
■ GPT-Datenträger (GUID-Partitionstabelle)	Ja	Ja
■ GPT-Startdatenträger (GUI-Partitionstabelle)	Nein	N/A
RAID-Datenträger *1:		
■ Software RAID (RAID-0 (Stripe))	Ja	Ja
■ Software RAID (RAID-1 (Gespiegelt))	Ja	Ja
■ Software RAID-5	Ja	Ja
■ Hardware RAID (schließt eingebettete RAID ein)	Ja	Ja
Dateisystem:		
■ EXT2	Ja	Ja
■ EXT3	Ja	Ja
■ EXT4	Ja	Ja
■ ReiserFS Version 3	Ja	Ja
Freigegebenes Volume:		
■ Windows-freigegebenes Volume	Nein	Ja
■ Windows NFS 3.0-Freigabe-Volume	Nein	Ja
■ Linux-freigegebenes Volume (Samba freigegeben)	Nein	Ja
■ Linux NFS-Freigabe	Nein	Ja
Gerätetyp:		
■ Wechseldatenträger (z. B. Memory Stick, RDX)	Ja	Ja

*1	Vom BIOS bereitgestellte Fake-RAID (auch als eingebettetes RAID bezeichnet) auf der Hauptplatine wird von Arcserve UDP Agent (Linux) nicht unterstützt.
	LVM (Logical Volume Manager) wird unter SUSE Linux Enterprise Server (SLES) 10 nicht unterstützt, jedoch wird LVM unter SLES 10 SP1 bis SP4 unterstützt. Ein eingebetteter LVM wird nicht unterstützt.

Sichern von mehr als 200 Knoten

Ein Sicherungsserver kann standardmäßig bis zu maximal 200 Knoten verwalten. Wenn mehr als 200 Knoten gesichert werden sollen, können Sie Mitglieds-Sicherungsserver einrichten. Verwalten Sie in diesem Fall alle Mitgliedsserver über einen zentralen Sicherungsserver.

Wenn Sie einen dedizierten Sicherungsserver verwenden und mehr als 200 Knoten sichern müssen, können Sie spezifische Einstellungen aktivieren und mehr als 200 Knoten verwalten.

Überprüfen der Voraussetzungen und Hinweise

Überprüfen Sie folgende Voraussetzungen, bevor Sie mehr als 200 Linux-Knoten sichern:

- Für den Sicherungsserver werden nur 64-Bit-Versionen von Linux unterstützt
- Beim Sicherungsserver muss es sich um einen dedizierten Server handeln. Arcserve UDP Agent (Linux) ändert die Systemeinstellungen, um den hohen Skalierbarkeitsanforderung des Servers gerecht zu werden.
- Der Server muss folgende Mindesthardwareanforderungen erfüllen. Wenn die Anzahl von Knoten höher ist, müssen die Hardware-Spezifikationen höher als die Mindestanforderungen sein.
  - 8 GB Speicher
  - 10 GB freier Speicher für den Ordner /opt

Überprüfen Sie die folgenden Hinweise:

- Wenn Sie Arcserve UDP Agent (Linux) für das Sichern von mehr als 200 Knoten aktivieren, verwendet der Server eine neue Datenbank (postgresql), um der hohen Skalierbarkeitsanforderung gerecht zu werden. Außer Jobübersicht und Aktivitätsprotokoll werden alle vorhandenen Knoten- und Jobinformation der alten Datenbank (sqlite) in die neue Datenbank migriert. Sie können nach der Migration nicht zur alten Datenbank (sqlite) zurückwechseln.
- Nach der Migration wird die Ausgabe für den Befehl d2djobhistory in einem anderen Format angezeigt.
- Als Best Practice sollten in einem Sicherungsjob weniger als 1000 Knoten gesichert werden.

Aktualisieren der TOMCAT-Konfigurationsdatei

Wenn Sie ein Upgrade von Arcserve UDP Agent (Linux) von einer Vorgängerversion wie r16.5 SP1 durchführen, aktualisieren Sie die TOMCAT-Konfigurationsdatei, damit die hohe Skalierbarkeitsanforderung des Sicherungsservers unterstützt wird. Mit dieser Aktualisierung können Sie mehr als 200 Knoten mit einem Sicherungsserver sichern.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Wechseln Sie zum Ordner bin:

   ```
   /opt/CA/d2dserver/bin
   ```

3. Stellen Sie sicher, dass keine Jobs ausgeführt werden, und halten Sie den Sicherungsserver danach mit folgendem Befehl an:

   ```
   d2dserver stop
   ```

   Wenn Jobs ausgeführt werden, warten Sie den Abschluss der Jobs ab, bevor Sie den Sicherungsserver anhalten.

4. Öffnen Sie die Datei "server.xml" von folgendem Speicherort:

   ```
   /opt/CA/d2dserver/TOMCAT/conf/
   ```

5. Aktualisieren Sie die folgenden Parameter.

   Wenn HTTPS verwendet wird, aktualisieren Sie folgende Parameter:

   ```
   <Connector port="8014" connectionTimeout="180000" protocol="HTTP/1.1"
   SSLEnabled="true" maxThreads="300"  acceptCount="200" scheme="https"
   secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

   Wenn HTTP verwendet wird, aktualisieren Sie folgende Parameter:

   ```
   <Connector connectionTimeout="180000" port="8014"
   maxThreads="300"  acceptCount="200" protocol="HTTP/1.1"/>
   ```

   Die globale TOMCAT-Konfigurationsdatei wurde erfolgreich aktualisiert.

6. Halten Sie den Sicherungsserver an.

   ```
   ./d2dserver stop
   ```

7. Führen Sie folgenden Befehl aus, um den Sicherungsserver zu starten:

   ```
   ./pgmgr init
   ```

   Dieser Befehl überprüft, dass alle notwendigen Änderungen abgeschlossen sind, und startet den Sicherungsserver.

```
[root@<Machine Name> bin]# ./d2dserver stop
arcserve UDP Agent(Linux) wurde angehalten.
[root@<Machine Name> bin]# ./pgmgr init
Der Installationsprozess wurde für die Postgresql-Datenbank gestartet. Das Debug
-Protokoll wird am folgenden Speicherort erstellt: /opt/CA/d2dserver/logs/pginit
.log.
Die Postgresql-Datenbank wurde erfolgreich installiert.
Daten wurden erfolgreich in die neue Datenbank migriert.
arcserve UDP Agent(Linux) wurde gestartet.
```

Sicherungsserver und Datenbankserver werden erfolgreich gestartet.

Verwalten des Datenbankservers

Über den Befehl *d2dserver start* wird üblicherweise der Datenbankserver gemeinsam mit dem Sicherungsserver gestartet. Wenn keine Jobs ausgeführt werden, werden mit dem Befehl *d2dserver stop* üblicherweise beide Server angehalten.

Wenn Sie den Datenbankserver manuell starten und anhalten möchten, können Sie folgende Befehle ausführen:

pgmgr start

Startet den Datenbankserver.

pgmgr stop

Hält den Datenbankserver an.

pgmgr status

Zeigt den Status des Datenbankservers an. Es wird angezeigt, ob der Datenbankserver ausgeführt wird oder angehalten wurde.

Hinweis: Wenn die Datenbank mit Daten überlastet ist, benötigt die Arcserve UDP Agent (Linux)-Konsole mehr Zeit, um Daten für Jobübersicht und Aktivitätsprotokoll zu laden. Informationen zum Verbessern der Datenabfrage finden Sie unter Verbessern der Abfrageleistung für Jobverlauf und Aktivitätsprotokoll.

Hinzufügen von Linux-Knoten zur Sicherung

Fügen Sie Linux-Knoten hinzu, sodass Sie diese Knoten an einem Sicherungsspeicherort sichern können. Linux-Knoten sind die Rechner, die Sie sichern möchten. Sie können Knoten manuell hinzufügen, oder Sie können ein Skript ausführen, um Knoten zu ermitteln und hinzuzufügen.

Gehen Sie wie folgt vor:

1. Geben Sie die URL des Sicherungsservers in einen Webbrowser ein, um die Benutzeroberfläche zu öffnen.

   Hinweis: Während der Installation von Arcserve UDP Agent (Linux) haben Sie die URL erhalten, um auf den Server zugreifen und ihn verwalten zu können.

2. Gehen Sie wie folgt vor, wenn Sie Knoten mithilfe eines Skripts ermitteln möchten:

   a. Klicken Sie im Menü "Knoten" auf "Hinzufügen", und wählen Sie "Discovery".

      Das Dialogfeld "Knoten-Discovery" wird geöffnet.

   b. Wählen Sie in der Drop-down-Liste "Skript" ein Skript.

      Hinweis: Weitere Informationen über das Erstellen des Skripts der Knoten-Discovery finden Sie unter "Ermitteln von Knoten mit einem Skript" in "So integrieren und automatisieren Sie Arcserve UDP Agent (Linux) in einer bestehenden IT-Umgebung".

   c. Geben Sie den "Ablaufplan" an, und klicken Sie auf "OK".

      Das Dialogfeld "Knoten-Discovery" wird geschlossen, und der Knoten-Discovery-Prozess wird gestartet. Die Registerkarte "Aktivitätsprotokoll" wird mit einer neuen Meldung aktualisiert.

3. Gehen Sie wie folgt vor, wenn Sie die einzelnen Knoten manuell hinzufügen möchten:

   a. Klicken Sie im Menü "Knoten" auf "Hinzufügen", und wählen Sie "Hostname/IP-Adresse".

      Das Dialogfeld "Knoten hinzufügen" wird geöffnet.

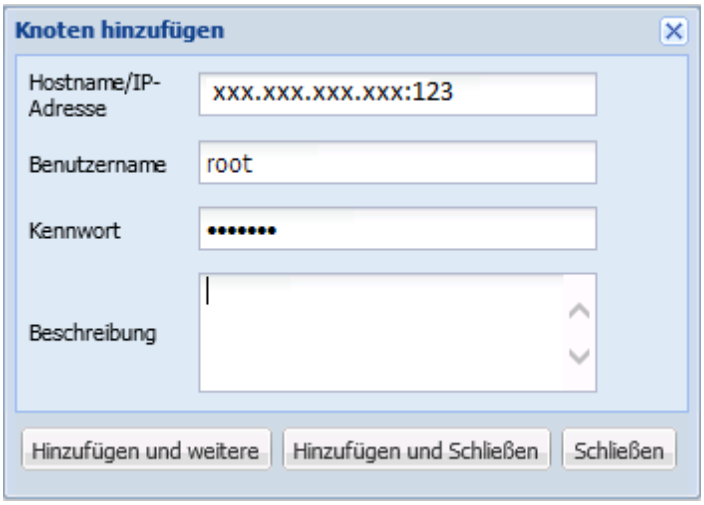
   b. Geben Sie den Hostnamen oder IP-Adresse des Linux-Knotens, den Namen des Benutzers, der über root-Berechtigungen verfügt, sowie das Kennwort ein.

      Hinweis: Wenn der standardmäßige SSH-Port des Knotens geändert wird, können Sie den Knoten wie folgt hinzufügen:

      `<IP-Name>:Portnummer`

      Beispiel: xxx.xxx.xxx.xxx:123

      In diesem Beispiel ist "xxx.xxx.xxx.xxx" die IP-Adresse und 123 die Portnummer.

   c. (Optional) Geben Sie eine Beschreibung des Knotens ein, damit Sie den Knoten einfacher finden können.

   d. Wählen Sie eine der folgenden Optionen.

      Hinzufügen und weitere

      Ermöglicht Ihnen, gleichzeitig mehrere Knoten hinzuzufügen. Nachdem Sie alle Knoten hinzugefügt haben, klicken Sie auf "Hinzufügen und Schließen" oder auf "Schließen", um das Dialogfeld "Knoten hinzufügen" zu schließen.

      Hinzufügen und Schließen

      Ermöglicht Ihnen, einen Knoten hinzuzufügen. Das Dialogfeld "Knoten hinzufügen" wird anschließend geschlossen.

      Schließen

      Schließt das Dialogfeld, ohne Knoten hinzuzufügen.

4. Klicken Sie auf die Registerkarte "Knoten", und stellen Sie sicher, dass die neuen Knoten darin aufgeführt sind.

Linux-Knoten werden für die Sicherung hinzugefügt.

(Optional) Vorbereiten des iSCSI-Volume als Sicherungsspeicher

Sie können Ihre Wiederherstellungspunkte auf einem Internet Small Computer System Interface-Volume (iSCSI) wiederherstellen. iSCSI wird verwendet, um Übertragung und Speicherung von Daten über ein Netzwerk, das den IP-Standard verwendet, zu verwalten.

Stellen Sie sicher, dass Sie die neueste Version der iSCSI-Initiator-Software auf Ihrem Sicherungsserver installiert haben. In RHEL-Systemen ist die Initiator-Software als "iscsi-initiator-utils" gepackt. In SLES-Systemen ist die Initiator-Software als "open-iscsi" gepackt.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Shell-Umgebung des Sicherungsquellknotens an.
2. Führen Sie einen der folgenden Befehle aus, um den iSCSI-Initiator-Daemon zu starten.
   - Für RHEL-Systeme:

     ```
     /etc/init.d/iscsid start
     ```

     In RHEL-Systemen heißt der Dienst "iscsid".
   - Für SLES-Systeme:

     ```
     /etc/init.d/open-iscsi start
     ```

     In SLES-Systemen heißt der Dienst "open-iscsi".
3. Führen Sie ein Discovery-Skript aus, um den iSCSI-Zielhost zu erkennen.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADRESSE>:<Portnummer>
   ```

   Der Standardportwert des iSCSI-Zielhost ist 3260.
4. Notieren Sie den iSCSI Qualified Name (IQN) des iSCSI-Zielhost, der durch das Discovery-Skript gefunden wird, bevor Sie sich manuell beim erkannten Zielcomputer anmelden.
5. Listen Sie das verfügbare Blockgerät des Sicherungsquellknotens auf.

   ```
   #fdisk -l
   ```
6. Melden Sie sich beim erkannten Ziel an.

   ```
   iscsiadm -m node -T <iSCSI Target IQN name> -p
   <ISCSI-SERVER-IP-ADRESSE>:<Portnummer>  -l
   ```

   Im Verzeichnis /dev des Sicherungsquellknotens wird ein Blockgerät angezeigt.

7. Führen Sie den folgenden Befehl aus, um den Namen des neuen Geräts abzurufen:

   ```
   #fdisk –l
   ```

   Im Sicherungsquellknoten können Sie ein zusätzliches Gerät, /dev/sd<x>, sehen.

   In diesem Beispiel ist der Name des Geräts "/dev/sdc". In den folgenden Schritten wird dieser Gerätename verwendet, um eine Partition und ein Dateisystem zu erstellen.

8. Formatieren Sie das iSCSI-Volume, und laden Sie es.
9. Erstellen Sie mithilfe der folgenden Befehle eine Partition und ein Dateisystem auf dem Sicherungsquellknoten.

   ```
   # fdisk /dev/sdc
   ```

   Wenn Sie nur eine Partition erstellt haben, verwenden Sie den folgenden Befehl, um ein Dateisystem für die einzelne Partition zu erstellen:

   ```
   # mkfs.ext3 /dev/sdc1
   ```

10. Laden Sie die neue Partition mithilfe der folgenden Befehle:

    ```
    # mkdir /iscsi
    # mount /dev/sdc1 /iscsi
    ```

    Die neue Partition wird geladen, und das iSCSI-Volume ist bereit, um als Sicherungsspeicher in einem Sicherungsjob verwendet zu werden.

11. (Optional) Fügen Sie folgenden Datensatz in den Ordner "/etc/fstab" hinzu, damit das iSCSI-Volume automatisch eine Verbindung zum Sicherungsserver herstellt, nachdem Sie den Server neu gestartet haben.

    ```
    /dev/sdc1 /iscsi ext3 _netdev 0 0
    ```

Das iSCSI-Volume ist bereit, um als Sicherungsspeicher verwendet zu werden.

Konfigurieren der Sicherungseinstellungen und erneutes Ausführen des Sicherungsjobs

Konfigurieren Sie die Sicherungseinstellungen mithilfe des Sicherungsassistenten. Sie können die Daten an einem Speicherort in einem NFS (Network File System), einem NAS (Network Attached Storage), einem CIFS (Common Internet File System) oder in einem lokalen Quellspeicherort speichern. Ein lokaler Quellspeicherort ist ein Speicherort im Sicherungsquellknoten, an dem die gesicherten Daten gespeichert werden. Der Sicherungsvorgang wird von einem Sicherungsjob initiiert. Der Sicherungsassistent erstellt den Sicherungsjob und führt den Job aus. Bei jedem erfolgreichen Ausführen einer Sicherung wird ein Wiederherstellungspunkt erstellt. Ein Wiederherstellungspunkt ist eine Zeitpunktkopie des Sicherungsknotens.

Auswählen der Sicherungsquelle

Geben Sie die Sicherungsquellknoten im Sicherungsassistenten an, sodass Sie diese Knoten an dem gewünschten Speicherort sichern können. Auf der Seite "Sicherungsquelle" des Sicherungsassistenten werden die Knoten angezeigt, die Sie sichern möchten. Verwenden Sie die Schaltfläche "Hinzufügen" auf dieser Seite, um weitere Knoten für die Sicherung hinzuzufügen.

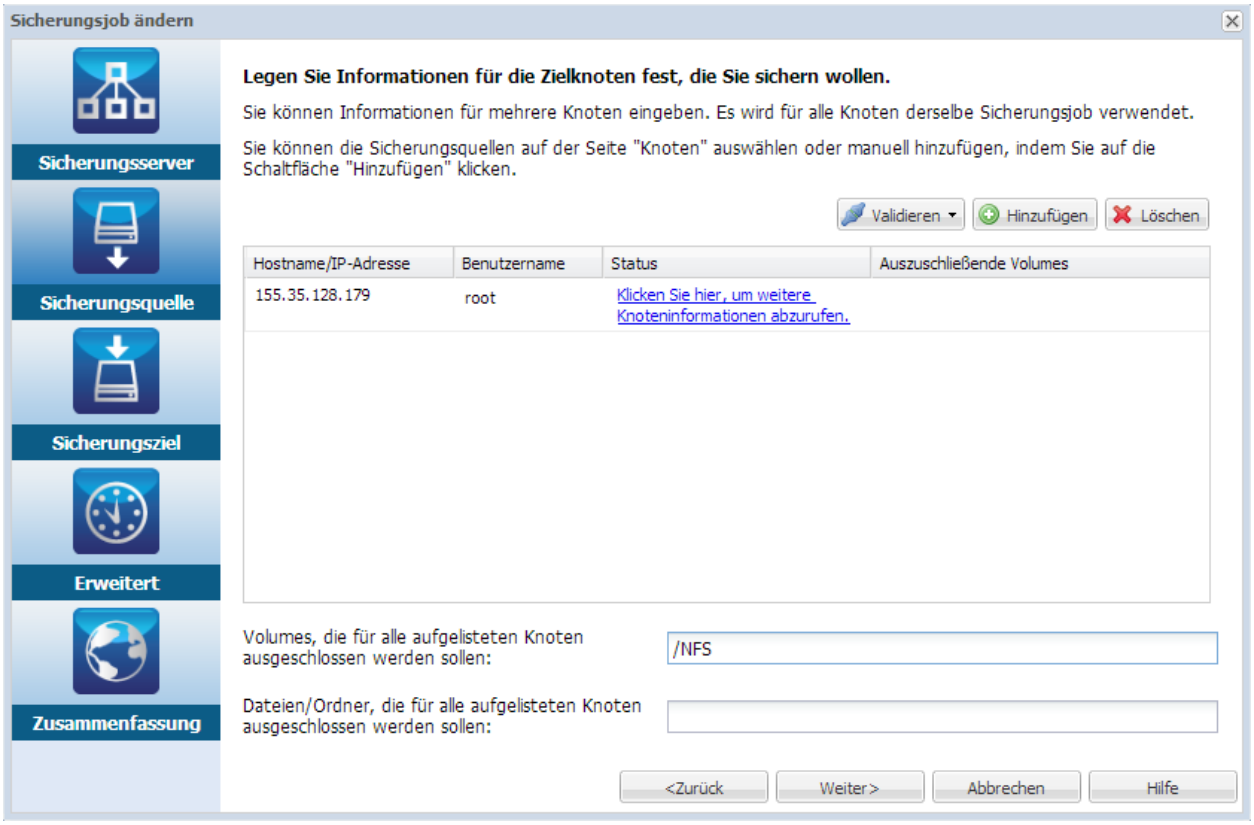
Hinweis: Wenn Sie den Sicherungsassistenten über die Schaltfläche "Ausgewählte Knoten sichern" öffnen, werden auf der Seite des Assistenten alle ausgewählten Knoten aufgelistet. Wenn Sie den Sicherungsassistenten über die Schaltfläche "Sichern" öffnen, werden die Knoten nicht auf der Seite des Assistenten aufgelistet. Sie müssen Knoten mithilfe der Schaltfläche "Hinzufügen" auf der Assistentenseite hinzufügen.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Knoten" die Knoten aus, die Sie sichern möchten.
2. Klicken Sie auf "Sichern", und wählen Sie im Menü "Assistent" die Option "Ausgewählte Knoten sichern" aus.

   Die Seite "Sicherungsserver" des Sicherungsassistenten wird geöffnet. Die Seite "Sicherungsserver" zeigt den Servernamen an.
3. Klicken Sie auf "Weiter".

   Die Seite "Sicherungsquelle" wird geöffnet. Die zuvor ausgewählten Knoten werden auf dieser Seite angezeigt.



4. (Optional) Klicken Sie auf der Seite "Sicherungsquelle" auf "Hinzufügen", um weitere Knoten hinzuzufügen, und geben Sie im Dialogfeld "Knoten hinzufügen" die Details ein.

5. (Optional) Klicken Sie auf das Symbol "Volumes ausschließen".

   Das Dialogfeld "Volume-Einstellungen ausschließen" wird geöffnet, in dem alle Volumes dieses Knotens aufgeführt sind.

6. (Optional) Wählen Sie die Kontrollkästchen für die Volumes aus, die nicht gesichert werden sollen, und klicken Sie auf "OK".

   Das Dialogfeld "Volume-Einstellungen ausschließen" wird geschlossen.

   Hinweis: Um ein bestimmtes Volume aus allen Sicherungsknoten auszuschließen, geben Sie die entsprechenden Bereitstellungspunktnamen in "**Volumes, die für alle aufgelisteten Knoten ausgeschlossen werden sollen**" an. Wenn Sie das Volume "*/*" oder das Volume "*/boot*" eines Knotens ausschließen, kann für diesen Knoten keine BMR ausgeführt werden.

7. (Optional) Geben Sie die Dateien/Ordner in "**Dateien/Ordner, die für alle aufgelisteten Knoten ausgeschlossen werden sollen**" ein.

   Die Dateien/Ordner sollten mit einem absoluten Pfadnamen angegeben und durch Doppelpunkte (:) voneinander abgetrennt werden. Platzhalterzeichen wie z. B. * und ? werden unterstützt und sollten nach dem letzten Schrägstrich des absoluten Pfadnamens verwendet werden. Wenn der Datei- bzw. Ordnername nach dem letzten Schrägstrich zwischen Klammern steht, werden diese Dateien/Ordner rekursiv ausgeschlossen. Andernfalls werden die Dateien/Ordner direkt ausgeschlossen.

   Beispiel:

   ```
   /home/user/a/foo*:/home/user/b/(foo*)
   ```

   Der erste Teil (home/user/a/foo*) hat die Ausschließung nur jener Dateien/Ordner unter "/home/user/a", die mit "foo*" übereinstimmen, zur Folge; Unterverzeichnisse werden allerdings gesichert. Der erste Teil (/home/user/b/(foo*) hat die Ausschließung aller Dateien/Ordner unter "/home/user/b", die mit "foo*" übereinstimmen, zur Folge; Unterverzeichnisse werden ebenfalls ausgeschlossen.

   Hinweise:

   - Wenn eine große Anzahl von Dateien/Ordnern eines Volumes ausgeschlossen wird, sollte das dazugehörige Volume ausgeschlossen werden.
   - Wenn viele Dateien/Ordnern ausgeschlossen werden, können Jobphase und -status beim Start des Sicherungsjobs lange "Volume wird gesichert" und "Aktiv" lauten.
   - Wenn der Wert in "**Dateien/Ordner, die für alle aufgelisteten Knoten ausgeschlossen werden sollen**" geändert wird, wird der Sicherungsjob in eine vollständige Sicherung konvertiert.

Wenn bestimmte Systemdateien von der Sicherung ausgeschlossen werden, kann das Linux-BS unter Umständen nicht gestartet werden, und die BMR-Funktion funktioniert nicht ordnungsgemäß. Diese Systemdateien sind, jedoch ausschließlich:

- Dateien und Ordner unter /bin, /sbin, /usr, /etc, /lib, /lib64, /boot, /var
- Die Ordner /proc, /sys, /dev, /tmp

Wenn Sie die Systemdateien ausschließen, sollten Sie die BMR-Funktion prüfen und sicherstellen, ob das Linux-BS ordnungsgemäß startet.

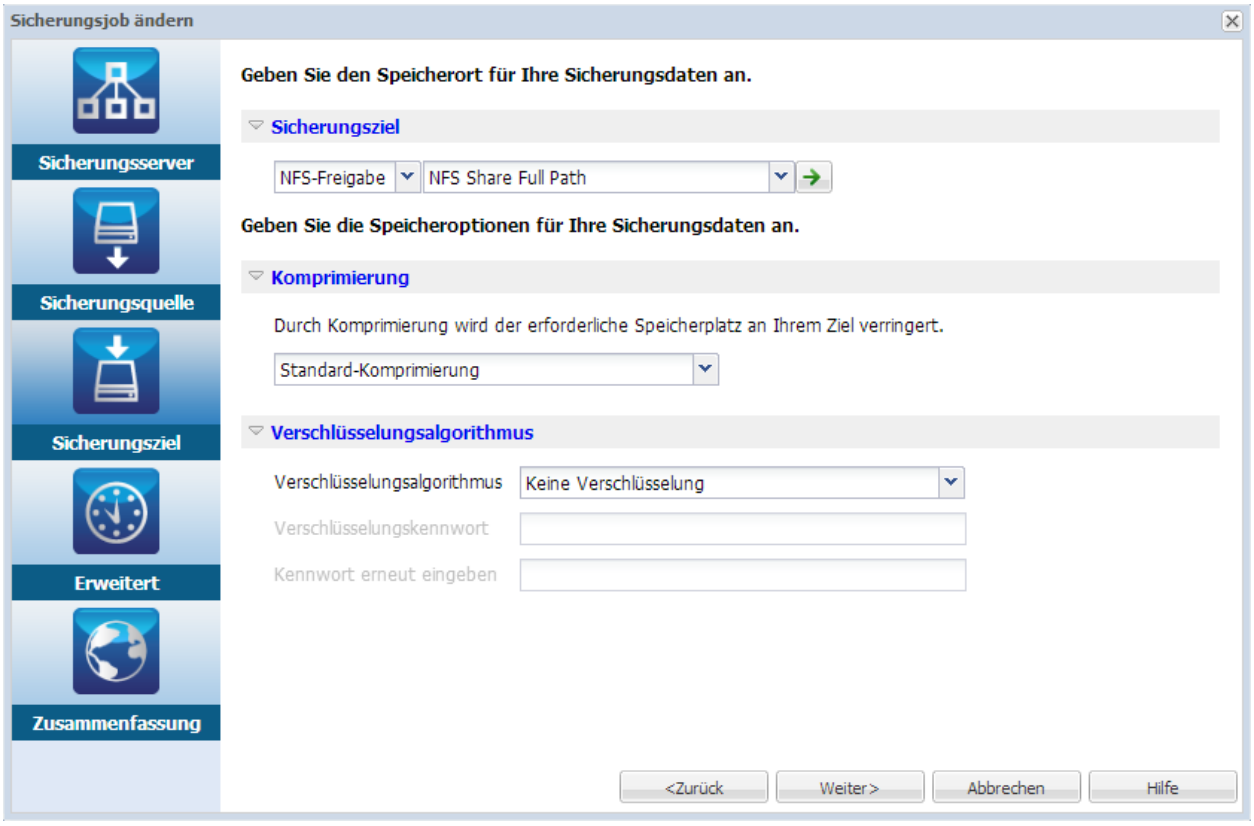
8. Klicken Sie auf "Weiter".

   Die Seite "Sicherungsziel" wird geöffnet.

Die Sicherungsquelle wird angegeben.

Auswählen des Sicherungsziels

Geben Sie auf der Seite "Sicherungsziel" des Sicherungsassistenten einen Speicherort an, an dem die gesicherten Daten (Wiederherstellungspunkte) gespeichert werden sollen. Das Sicherungsziel kann eine NFS-Freigabe, eine CIFS-Freigabe oder eine lokale Quelle sein. "Quelle - lokal" ist der Sicherungsquellknoten. Wenn Ihr Sicherungsziel "Quelle - lokal" ist, dann werden die Sicherungsdaten direkt auf dem eigenen lokalen Datenträger abgespeichert.



Wenn ein physischer Datenträger zwei logische Volumes einschließt, können Sie ein Volume als die Sicherungsquelle und das andere Volume als das Sicherungsziel angeben.

Hinweis: Wenn Sie "Quelle - lokal" als Sicherungsziel auswählen, kann der Sicherungsserver die Wiederherstellungspunkte nicht verwalten. Informationen zum Verwalten der Wiederherstellungssätze finden Sie unter "Verwalten der Wiederherstellungssätze" in "So verwalten Sie die Einstellungen des Sicherungsservers".

Gehen Sie wie folgt vor:

1. Wählen Sie ein Ziel aus der Drop-down-Liste "Sicherungsziel", und geben Sie den vollständigen Pfad des Speicherorts an.

   - Wenn Sie "NFS-Freigabe" ausgewählt haben, geben Sie die Details für das Sicherungsziel im folgenden Format ein:
     `IP-Adresse der NFS-Freigabe:/vollständiger Pfad des Speicherorts`

     Hinweis: Einige Versionen des Data Domain-NAS unterstützen den Mechanismus der Dateisperre von NFS nicht. Dadurch können solche NFS-Freigaben nicht als Sicherungsziel verwendet werden. Weitere Informationen zu diesem Problem finden Sie in den Versionshinweisen unter "Kompatibilitätsprobleme mit Arcserve UDP Agent (Linux)".

   - Wenn Sie "CIFS-Freigabe" ausgewählt haben, geben Sie die Details für das Sicherungsziel im folgenden Format ein:
     `//Hostname/Freigabeordner`

     Hinweis: Der freigegebene Ordnername darf keine Leerzeichen enthalten.

   - Wenn Sie "Quelle - lokal" ausgewählt haben, müssen Sie einige Einstellungen ändern, sodass der Sicherungsserver die Wiederherstellungspunkte verwalten kann. Berücksichtigen Sie zum Beispiel "server-A" als Hostnamen des Sicherungsservers und "node-B" als Hostnamen des Quellknotens. Gehen Sie dann wie folgt vor, um die Einstellungen für "node-B" zu ändern:

     - Stellen Sie sicher, dass der NFS-Server ausgeführt wird. Sie können den folgenden Befehl ausführen, um den NFS-Serverstatus zu überprüfen:

       service nfs status

     - Wenn der NFS-Server nicht ausführt wird, führen Sie den folgenden Befehl aus, um den NFS-Server zu starten:

       service nfs start

     - Wenn das Zielverzeichnis der Sicherung auf "node-B" */backup/test* ist, fügen Sie folgende Zeile zu */etc/exports* hinzu:

       /backup/test server-A(rw,no_root_squash)

       Führen Sie nun den folgenden Befehl aus:

       exportfs -a

     - Fügen Sie in der Benutzeroberfläche des Sicherungsservers *node-B:/backup/test* als Speicherort für die Sicherung hinzu. Der Speicherort der lokalen Quelle wird in der Drop-down-Liste "Sicherungsziel" angezeigt.

2. Klicken Sie auf die Pfeilschaltfläche, um die Sicherungsziel-Informationen zu validieren.

   Wenn das Sicherungsziel ungültig ist, wird eine Fehlermeldung angezeigt.

3. Wählen Sie eine Komprimierungsebene aus der Drop-down-Liste Komprimierung, um den für die Sicherung verwendeten Komprimierungstyp anzugeben.

   Die verfügbaren Optionen für Komprimierung sind:

   Standard-Komprimierung

   Gibt an, dass diese Option ein Gleichgewicht zwischen CPU-Auslastung und verwendetem Speicherplatz bereitstellt. Dieser Komprimierungstyp ist die Standardeinstellung.

   Maximale Komprimierung

   Diese Option bedeutet höchste CPU-Auslastung (niedrigste Geschwindigkeit), aber auch niedrigste Speicherplatzverwendung für Ihr Sicherungs-Image.

4. Wählen Sie einen Algorithmus aus der Drop-down-Liste Verschlüsselungsalgorithmus aus, und geben Sie bei Bedarf das Verschlüsselungskennwort ein.

   a. Wählen Sie den Verschlüsselungsalgorithmus aus, den Sie für Sicherungen verwenden möchten.

      Bei der Datenverschlüsselung werden Daten in ein Format umgewandelt, das ohne den entsprechenden Entschlüsselungsmechanismus nicht verständlich ist. Der Datenschutz von Arcserve UDP Agent (Linux) verwendet sichere AES- (Advanced Encryption Standard) Verschlüsselungsalgorithmen, um maximale Sicherheit und Datenschutz Ihrer angegebenen Daten zu erreichen.

      Die verfügbaren Formatoptionen sind "Keine Verschlüsselung", "AES-128", "AES-192" und "AES-256". (Um die Verschlüsselung zu deaktivieren, wählen Sie "Keine Verschlüsselung" aus).

      - Eine vollständige Sicherung und alle verknüpften Zuwachssicherungen müssen den gleichen Verschlüsselungsalgorithmus verwenden.
      - Wenn sich der Verschlüsselungsalgorithmus für eine Zuwachssicherung geändert hat, müssen Sie eine vollständige Sicherung ausführen.

        Wenn Sie zum Beispiel das Algorithmusformat ändern und dann eine Zuwachssicherung ausführen, wird der Sicherungstyp dann automatisch in eine vollständige Sicherung konvertiert.

   b. Wenn ein Verschlüsselungsalgorithmus ausgewählt wird, müssen Sie ein Verschlüsselungskennwort angeben (und es bestätigen).

      - Das Verschlüsselungskennwort kann höchstens aus 23 Zeichen bestehen.
      - Eine vollständige Sicherung und alle verknüpften Zuwachssicherungen verwenden das gleiche Kennwort zur Datenverschlüsselung.

5. Klicken Sie auf "Weiter".

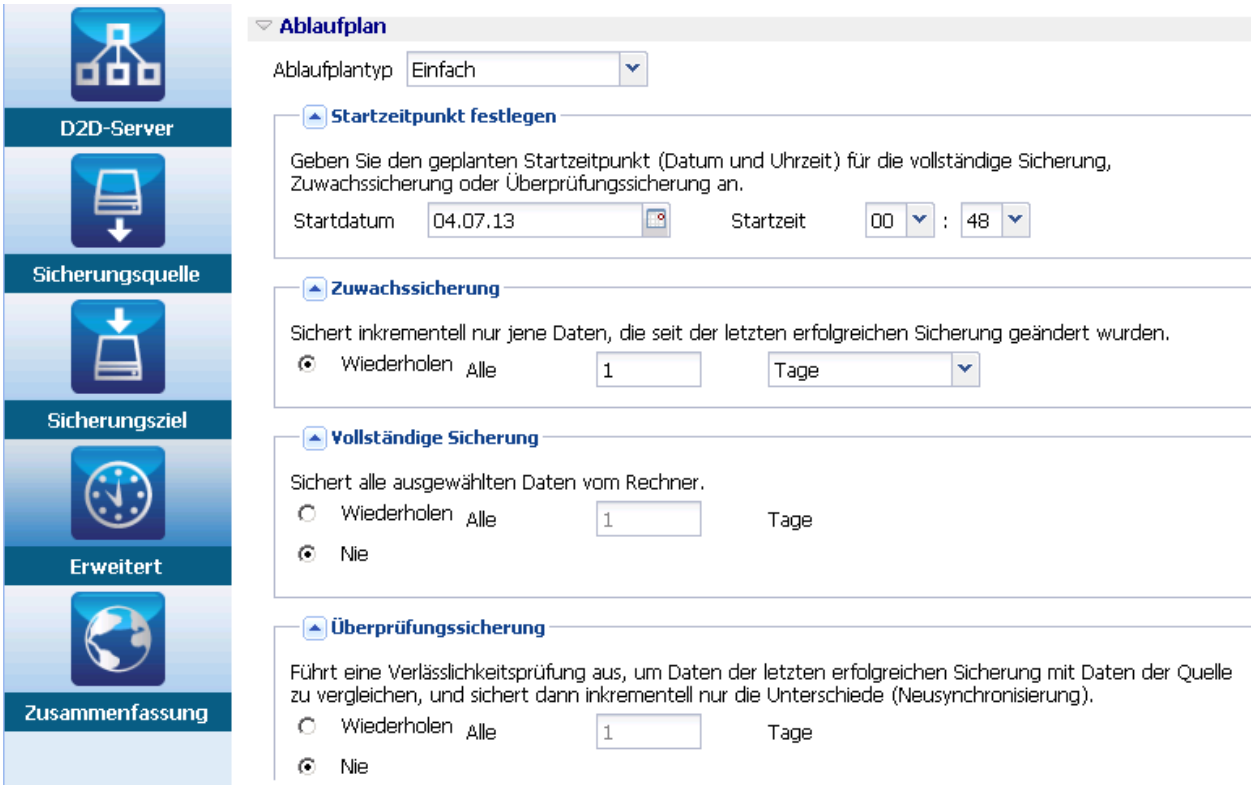
   Das Dialogfeld "Erweitert" wird geöffnet.

Das Sicherungsziel wird angegeben.

Festlegen von erweiterten Einstellungen

Geben Sie den Sicherungsablaufplan, die Einstellungen für den Wiederherstellungssatz sowie die Einstellungen für Vorsicherung und Nachsicherung auf der Seite "Erweitert" an.

Folgendes Diagramm zeigt die Seite Erweitert des Sicherungsassistenten an. In diesem Diagramm ist die Option Keine für den Ablaufplantyp aktiviert.



Folgende Einstellungen sind auf der Seite Erweitert verfügbar:

- Die Ablaufplan-Einstellungen stellen sicher, dass der Sicherungsjob regelmäßig zu einer angegebenen Zeit ausgeführt wird.
- Die Einstellungen des Wiederherstellungssatzes stellen sicher, dass eine periodische Wartung der Wiederherstellungssätze erfolgt. Wenn die Anzahl von Wiederherstellungssätzen die angegebene Zahl überschreitet, wird der älteste Wiederherstellungssatz gelöscht, um angegebene Zahl zu jedem Zeitpunkt beizubehalten.
- Über die Einstellung Sicherung drosseln können Sie die Höchstgeschwindigkeit (MB/Min.), in der die Sicherungen geschrieben werden, aktivieren und angeben.
- Die Einstellungen für Prä-/Post-Skripts definieren die Skripte, die auf dem Sicherungsserver und dem Zielknoten ausgeführt werden können. Sie können die Skripte konfigurieren, um bestimmte Aktionen vor dem Beginn eines Jobs, während der Ausführung des Jobs oder nach dem Abschluss des Jobs auszuführen.

Um die Verwaltung Ihrer Wiederherstellungspunkte zu optimieren, sollten Sie folgende Empfehlungen beachten, wenn Sie die Häufigkeit Ihrer Sicherungen planen:

- Für Systeme, die durch Zuwachssicherungen, die alle 15 Minuten ausgeführt werden, geschützt sind, sollten Sie eine wöchentliche vollständige Sicherung planen (um Ihr Basis-Image zu aktualisieren).
- Für Systeme, die durch stündliche Zuwachssicherungen geschützt sind, sollten Sie eine monatliche vollständige Sicherung planen (um Ihr Basis-Image zu aktualisieren).

Hinweis: Wenn der verwendete Speicherplatz für das Speichern Ihrer Sicherungs-Images ein Problem darstellt, dann sollten Sie überlegen, vollständige Sicherungen weniger häufig zu planen, um weniger Speicherplatz zu nutzen.

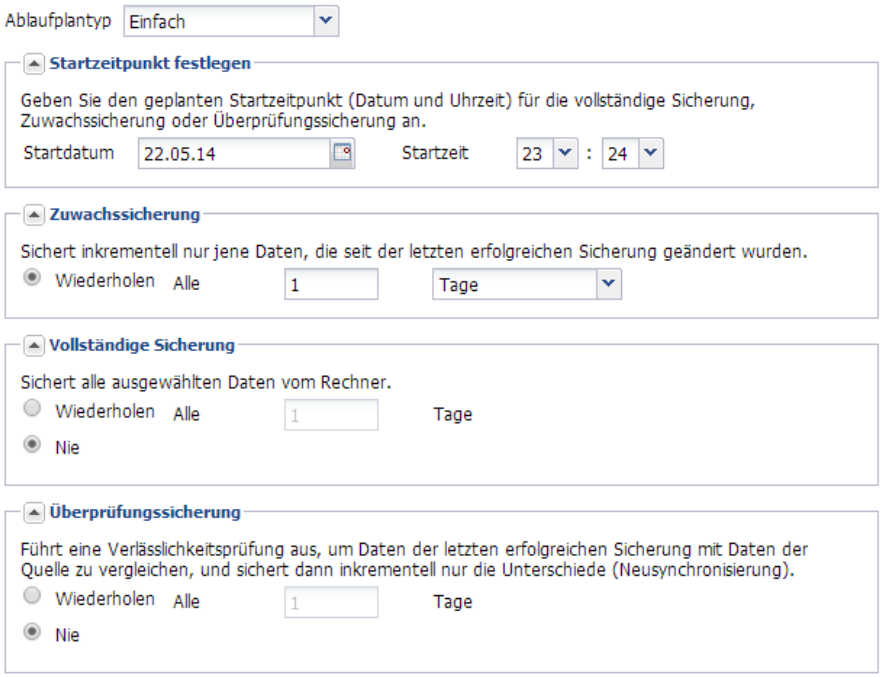
Gehen Sie wie folgt vor:

1. Legen Sie das Startdatum und die Uhrzeit fest, indem Sie eine der folgenden Optionen in der Drop-down-Liste Ablaufplantyp auswählen:

   Einfach

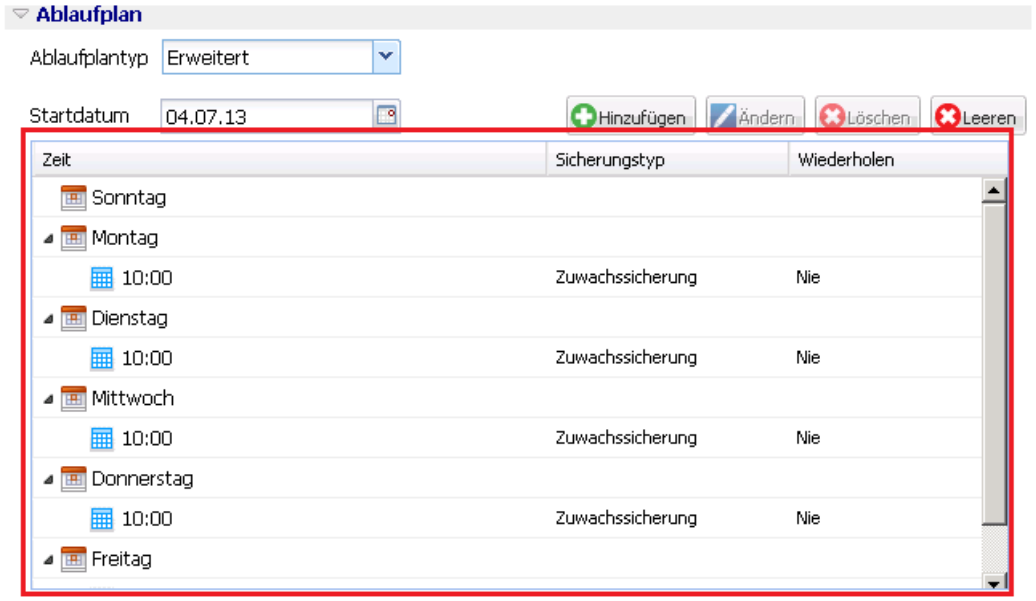
   Wählen Sie die Option Einfach aus, um die Zuwachssicherung, Vollständige Sicherung und Überprüfungssicherung für das angegebene Startdatum und die Startzeit zu planen. Für jeden Sicherungstyp können Sie auch die Wiederholungsdauer für eine Sicherung angeben, oder Sie können angeben, dass Sicherungen niemals wiederholt werden sollen. Das Startdatum und die Startzeit sind für alle Sicherungstypen festgelegt. Sie können also kein anderes Startdatum und keine andere Startzeit für verschiedene Sicherungstypen angeben.

   Hinweis: Weitere Informationen zu den Sicherungstypen finden Sie unter *Funktionsweise der Sicherungstypen*.



Erweitert

Wählen Sie die Option Erweitert aus, um jeden Wochentag mehrere Sicherungsablaufpläne anzugeben. Sie können also ein anderes Startdatum und eine andere Startzeit für verschiedene Sicherungstypen angeben. Sie können den erweiterten Ablaufplan hinzufügen, ändern, löschen und leeren. Wenn Sie auf Leeren klicken, werden alle erweiterten Sicherungsablaufpläne aus der Taskleiste des erweiterten Ablaufplans gelöscht.



Erweiterter Ablaufplan

Um einen Sicherungsablaufplan hinzuzufügen, führen Sie diese Schritte aus:

a. Klicken Sie auf "Hinzufügen".

Das Dialogfeld "Sicherungsablaufplan hinzufügen" wird geöffnet.

b. Geben Sie Ihre Sicherungsablaufplanoptionen an, und klicken Sie auf "OK".

Der angegebene Sicherungsablaufplan wird auf der Taskleiste des erweiterten Ablaufplans angezeigt.

Keine

Wählen Sie die Option "Keine" aus, um den Sicherungsjob zu erstellen und um den Job in der Registerkarte Jobstatus zu speichern. Diese Option wird den Job nicht ausführen, da kein angegebener Ablaufplan vorhanden ist. Wenn Sie den Job übergeben, wird der Status des Jobs in den Status Bereit geändert. Wenn Sie den Job ausführen möchten, müssen Sie den Job auswählen im Menü "Job" die Option "Jetzt ausführen" wählen. Immer, wenn Sie den Job ausführen möchten, müssen Sie dies manuell vornehmen. Sie können auch ein Skript schreiben, um diesen Job nach einem eigenen Ablaufplan auszuführen.

2. Geben Sie die Einstellungen für den Wiederherstellungssatz an.

Hinweis: Weitere Informationen zu den Wiederherstellungssätzen finden Sie unter *Funktionsweise der Wiederherstellungssätze*.

Geben Sie die Anzahl der Wiederherstellungssätze an, die aufbewahrt werden sollen

Gibt die Anzahl der aufbewahrten Wiederherstellungssätze an.

Einen neuen Wiederherstellungssatz starten jeden::

Ausgewählten Tag der Woche

Gibt den Wochentag an, der für das Starten eines neuen Wiederherstellungssatzes ausgewählt wurde.

Ausgewählten Tag des Monats

Gibt den Monatstag an, der für das Starten eines neuen Wiederherstellungssatzes ausgewählt wurde. Geben Sie einen Wert zwischen 1 und 30 an, oder geben Sie den letzten Tag des Monats an.

Hinweis: Der Sicherungsserver überprüft alle 15 Minuten die Wiederherstellungssätze im konfigurierten Sicherungsspeicher und löscht alle zusätzlichen Wiederherstellungssätze aus dem Sicherungsspeicherort.

3. Legen Sie den Wert zum Drosseln der Sicherung fest.

   Sie können die Höchstgeschwindigkeit festlegen (MB/Min), mit der Sicherungen geschrieben werden. Sie können die Sicherungsgeschwindigkeit drosseln, um die CPU- oder Netzwerkauslastung zu reduzieren. Allerdings wirkt sich die Einschränkung der Sicherungsgeschwindigkeit negativ auf das Sicherungsfenster aus. Wenn Sie die Höchstgeschwindigkeit für Sicherungen senken, dauert es länger, die Sicherung abzuschließen. Für einen Sicherungsjob wird auf der Registerkarte Jobstatus die durchschnittliche Lese- und Schreibgeschwindigkeit des Jobs angezeigt, der ausgeführt wird, sowie die Begrenzung, die für die Drosselung der Geschwindigkeit konfiguriert ist.

   Hinweis: Standardmäßig ist die Option "Sicherung drosseln" nicht aktiviert und die Sicherungsgeschwindigkeit wird nicht gesteuert.

4. Geben Sie Ihre Prä-/Post-Sicherungseinstellungen in Einstellungen für Prä-/Post-Skripts an.

   Diese Skripte führen Skriptbefehle für Aktionen aus, die vor dem Start des Jobs und/oder nach Abschluss des Jobs durchgeführt werden sollen.

   Hinweis: Die Felder für die Prä-/Post-Skripteinstellung werden nur aufgefüllt, wenn Sie bereits eine Skriptdatei erstellt und unter folgendem Speicherort platziert haben:

   ```
   /opt/CA/d2dserver/usr/prepost
   ```

   Hinweis: Weitere Informationen zur Erstellung der Prä-/Post-Skripte finden Sie unter *Verwalten der Prä-/Post-Skripte für Automatisierung*.

5. Klicken Sie auf "Weiter".

   Die Seite "Zusammenfassung" wird geöffnet.

Der erweiterte Ablaufplan wird angegeben.

Hinweis: Wenn für denselben Zeitpunkt mehrere Sicherungstypen geplant sind, gelten die folgenden Prioritäten:

- Priorität 1 - Vollständige Sicherung
- Priorität 2 - Überprüfungssicherung
- Priorität 3 - Zuwachssicherung

Wenn z. B. alle drei Sicherungstypen für denselben Zeitpunkt geplant sind, führt Arcserve UDP Agent (Linux) eine vollständige Sicherung durch. Wenn keine vollständige Sicherung, aber eine Überprüfungssicherung und eine Zuwachssicherung geplant sind, führt Arcserve UDP Agent (Linux) die Überprüfungssicherung durch. Eine geplante Zuwachssicherung wird nur dann durchgeführt, wenn keine Konflikte mit anderen Sicherungstypen bestehen.

Funktionsweise der Sicherungstypen

Auf der Seite Erweitert des Sicherungsassistenten können Sie folgende Sicherungstypen angeben:

Zuwachssicherung

Es werden nur die Blöcke gesichert, die seit der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Arcserve Unified Data Protection Agent for Linux verwendet einen Treiber, um die geänderten Blöcke im Quellknoten seit der letzten erfolgreichen Sicherung zu überwachen.

Es stehen die Optionen "Wiederholen" und "Nie" zur Verfügung. Wenn Sie "Wiederholen" auswählen, müssen Sie auch die Zeitspanne (Minuten, Stunden oder Tage) zwischen den Sicherungsversuchen festlegen.

Minimum: 15 Minuten

Standard: 1 Tag

Vollständige Sicherung

Sichert den gesamten Quellknoten. Je nach der Volumegröße des Sicherungsknotens wird bei einer vollständigen Sicherung ein großes Sicherungs-Image erstellt, und die Sicherung nimmt längere Zeit in Anspruch. Es stehen die Optionen "Wiederholen" und "Nie" zur Verfügung.

Wenn Sie "Wiederholen" auswählen, müssen Sie auch die Zeitspanne (Minuten, Stunden oder Tage) zwischen den Sicherungsversuchen festlegen.

Minimum: 1 Tag

Standard: Nie (keine geplante Wiederholung)

Überprüfungssicherung

Überprüft die Gültigkeit und Vollständigkeit der geschützten Daten durch einen Vergleich des gespeicherten Sicherungs-Images mit der ursprünglichen Sicherungsquelle. Im Bedarfsfall wird das Image neu synchronisiert. Bei einer Überprüfungssicherung wird die letzte Sicherung jedes einzelnen Blocks mit den Inhalten und Informationen der Quelle verglichen. Dieser Vergleich stellt sicher, dass die letzten gesicherten Blöcke den jeweiligen Quellinformationen entsprechen. Wenn das Sicherungs-Image eines Blocks nicht der Quelle entspricht (wahrscheinlich aufgrund von Änderungen seit der letzten Sicherung), aktualisiert Arcserve Unified Data Protection Agent for Linux die Sicherung dieses Blocks (Neusynchronisierung). In sehr seltenen Fällen kann eine Überprüfungssicherung auch durchgeführt werden, um eine vollständige Sicherung zu erhalten, ohne den erforderlichen Speicherplatz einer vollständigen Sicherung zu verwenden.

Vorteile: Im Vergleich zu einer vollständigen Sicherung wird ein nur ein kleines Sicherungs-Image erstellt, da nur die geänderten Blöcke (Blöcke, die nicht mit der letzten Sicherung übereinstimmen) gesichert werden.

Nachteile: Die Sicherung benötigt viel Zeit, da alle Quellenblöcke mit den Blöcken der letzten Sicherung verglichen werden.

Es stehen die Optionen "Wiederholen" und "Nie" zur Verfügung. Wenn Sie "Wiederholen" auswählen, müssen Sie auch die Zeitspanne (Minuten, Stunden oder Tage) zwischen den Sicherungsversuchen festlegen.

Minimum: 1 Tag

Standard: Nie (keine geplante Wiederholung)

Welche Art von Sicherung ausgeführt wird, hängt von den folgenden Situationen ab:

- Wenn Sie die Sicherung für die ausgewählten Knoten zum ersten Mal ausführen, ist die erste Sicherung immer eine vollständige Sicherung.
- Wenn Sie den Sicherungsjob für den gleichen Satz von Knoten erneut ausführen und das Sicherungsziel ebenfalls das gleiche ist, ist der Sicherungstyp eine Zuwachssicherung.
- Wenn Sie den Sicherungsjob für den gleichen Satz von Knoten ausführen, das Sicherungsziel jedoch ein anderes ist, ist der Sicherungstyp eine vollständige Sicherung. Das liegt daran, dass Sie das Sicherungsziel geändert haben und dies für das neue Ziel die erste Sicherung ist. Die erste Sicherung ist immer eine vollständige Sicherung.

- Wenn Sie einen Knoten löschen und den gleichen Knoten erneut hinzufügen, Sie das Sicherungsziel jedoch nicht ändern, ist die Sicherung eine Überprüfungssicherung. Dies liegt daran, dass Sie diesen Knoten bei den früheren Sicherungsjobs gesichert haben. Wenn Sie den Knoten löschen und dann erneut hinzufügen, überprüft der Sicherungsjob alle Blöcke dieses Knotens mit dem letzten Sicherungs-Image. Wenn der Sicherungsjob zu dem Schluss gelangt, dass es sich um den gleichen Knoten handelt, werden nur die geänderten Blöcke gesichert. Wenn der Sicherungsjob kein Sicherungs-Image dieses Knotens im Sicherungsziel findet, ist der Sicherungstyp eine vollständige Sicherung.

Funktionsweise der Wiederherstellungssätze

Ein Wiederherstellungssatz ist eine Speichereinstellung, bei der eine Gruppe von Wiederherstellungspunkten, die über einen angegebenen Zeitraum gesichert wurden, als ein Satz gespeichert wird. Ein Wiederherstellungssatz umfasst eine Serie von Sicherungen, beginnend bei einer vollständigen Sicherung, gefolgt von einer Reihe von Zuwachs-, Überprüfungs- oder vollständigen Sicherungen. Sie können die Anzahl der Wiederherstellungssätze angeben, die beibehalten werden soll.

Die "Einstellungen des Wiederherstellungssatzes" stellen sicher, dass eine periodische Wartung der Wiederherstellungssätze erfolgt. Wenn das angegebene Limit überschritten ist, wird der älteste Wiederherstellungssatz gelöscht. Folgende Werte definieren die standardmäßigen, die minimalen und die maximalen Wiederherstellungssätze in Arcserve UDP Agent (Linux):

Standard: 2

Minimum: 1

Höchstanzahl von aufzubewahrenden Wiederherstellungssätze: 100

Die Höchstanzahl der Wiederherstellungspunkte (einschließlich einer vollständigen Sicherung): 1344

Hinweis: Wenn Sie einen Wiederherstellungssatz löschen möchten, um Sicherungsspeicherplatz zu sparen, reduzieren Sie die Anzahl der aufbewahrten Sätze, und der Sicherungsserver löscht automatisch den ältesten Wiederherstellungssatz. Versuchen Sie nicht, den Wiederherstellungssatz manuell zu löschen.

Beispiel-Satz 1:

- Vollständige Sicherung
- Zuwachssicherung
- Zuwachssicherung

- Überprüfen
- Zuwachssicherung

Beispiel-Satz 2:

- Vollständige Sicherung
- Zuwachssicherung
- Vollständige Sicherung
- Zuwachssicherung

Eine vollständige Sicherung ist erforderlich, um einen neuen Wiederherstellungssatz zu starten. Die Sicherung, die den Satz startet, wird automatisch in eine vollständige Sicherung konvertiert, auch wenn keine vollständige Sicherung zur Ausführung zu diesem Zeitpunkt konfiguriert oder geplant ist. Nachdem die Einstellung des Wiederherstellungssatzes geändert wurde (zum Beispiel wenn der Ausgangspunkt des Wiederherstellungssatzes der ersten Sicherung von Montag auf die erste Sicherung von Donnerstag geändert wird), dann wird der Ausgangspunkt der vorhandenen Wiederherstellungssätze nicht geändert.

Hinweis: Ein unvollständiger Wiederherstellungssatz wird nicht mitgezählt, wenn ein vorhandener Wiederherstellungssatz berechnet wird. Ein Wiederherstellungssatz wird nur als vollständig erachtet, wenn die Anfangssicherung des nächsten Wiederherstellungssatzes erstellt wird.

Beispiel 1: Aufbewahren von einem Wiederherstellungssatz:

- Legen Sie die Zahl der Wiederherstellungssätze, die aufbewahrt werden sollen, auf 1 fest.

  Der Sicherungsserver bewahrt immer zwei Sätze auf, um einen vollständigen Satz beizubehalten, bevor der nächste Wiederherstellungssatz gestartet wird.

Beispiel 2 - Aufbewahren von 2 Wiederherstellungssätzen:

- Legen Sie die Zahl der Wiederherstellungssätze, die aufbewahrt werden sollen, auf 2 fest.

  Der Sicherungsserver löscht den ersten Wiederherstellungssatz, wenn der vierte Wiederherstellungssatz dabei ist, zu starten. Dadurch wird sichergestellt, dass, wenn die erste Sicherung gelöscht und die vierte Sicherung gestartet wird, noch zwei verfügbare Wiederherstellungssätze (Wiederherstellungssatz 2 und Wiederherstellungssatz 3) auf dem Datenträger vorhanden sind.

  Hinweis: Auch wenn Sie nur einen Wiederherstellungssatz aufbewahren möchten, benötigen Sie Speicherplatz für mindestens zwei vollständige Sicherungen.

Beispiel 3 - Aufbewahren von 3 Wiederherstellungssätzen:

- Die Startzeit der Sicherung ist 06:00 Uhr, 20. August 2012.
- Eine Zuwachssicherung wird alle 12 Stunden ausgeführt.
- Ein neuer Wiederherstellungssatz beginnt bei der letzten Sicherung am Freitag.
- Sie möchten 3 Wiederherstellungssätze aufbewahren.

Mit der obigen Konfiguration wird jeden Tag eine Zuwachssicherung um 06:00 Uhr und um 18:00 Uhr ausgeführt. Der erste Wiederherstellungssatz wird erstellt, wenn die erste Sicherung (muss eine vollständige Sicherung sein) durchgeführt wurde. Dann wird die erste vollständige Sicherung als die Anfangssicherung des Wiederherstellungssatzes markiert. Wenn die am Freitag um 18:00 Uhr geplante Sicherung ausgeführt wird, dann wird diese Sicherung in eine vollständige Sicherung konvertiert und als gestartete Sicherung des Wiederherstellungssatzes markiert.

(Optional) Verwalten der Prä-/Post-Skripte für Automatisierung

Mit Prä-/Post-Skripts können Sie Ihre eigene Geschäftslogik in bestimmten Phasen eines in Bearbeitung befindlichen Jobs ausführen. Sie können in **Einstellungen vor/nach dem Skript** des **Sicherungsassistenten** und des **Wiederherstellungsassistenten** auf der Benutzeroberfläche angeben, wann Ihre Skripte ausgeführt werden sollen. Die Skripts können je nach Einstellung auf dem Sicherungsserver ausgeführt werden.

Das Verwalten von Prä-/Post-Skripts ist ein zweiteiliger Vorgang, der das Erstellen des Prä-/Post-Skripts und das Einfügen des Skripts in den "prepost"-Ordners umfasst.

Erstellen von Prä-/Post-Skripts

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Erstellen Sie eine Skriptdatei, indem Sie die Umgebungsvariablen in Ihrer bevorzugten Skripterstellungssprache verwenden.

   Umgebungsvariablen des Prä-/Post-Skripts

   Verwenden Sie die folgenden Umgebungsvariablen, um Ihr Skript zu erstellen:

   D2D_JOBNAME

   Gibt den Namen des Jobs an.

D2D_JOBID

Gibt die Job-ID an. Die Job-ID ist eine Nummer, die für den Job vergeben wird, wenn Sie den Job ausführen. Wenn Sie den gleichen Job erneut ausführen, erhalten Sie eine neue Jobnummer.

D2D_TARGETNODE

Identifiziert den Knoten, der gesichert oder wiederhergestellt wird.

D2D_JOBTYPE

Identifiziert den Typ des ausgeführten Jobs. Die folgenden Werte identifizieren die D2D_JOBTYPE-Variable:

backup.full

Identifiziert den Job als eine vollständige Sicherung.

backup.incremental

Identifiziert den Job als eine Zuwachssicherung.

backup.verify

Identifiziert den Job als eine Überprüfungssicherung.

restore.bmr

Identifiziert den Job als eine Bare-Metal-Recovery (BMR). Dies ist ein Wiederherstellungsjob.

restore.file

Identifiziert den Job als eine Wiederherstellung auf Dateiebene. Dies ist ein Wiederherstellungsjob.

D2D_SESSIONLOCATION

Identifiziert den Speicherort, an dem die Wiederherstellungspunkte gespeichert sind.

D2D_PREPOST_OUTPUT

Identifiziert eine Temp-Datei. Der Inhalt der Anfangszeile der Temp-Datei wird im Aktivitätsprotokoll angezeigt.

D2D_JOBSTAGE

Gibt die Phase des Jobs an. Die folgenden Werte identifizieren die D2D_JOBSTAGE-Variable:

pre-job-server

Identifiziert das Skript, das auf dem Sicherungsserver ausgeführt wird, bevor der Job startet.

post-job-server

Identifiziert das Skript, das auf dem Sicherungsserver ausgeführt wird, nachdem der Job abgeschlossen ist.

pre-job-target

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, bevor der Job startet.

post-job-target

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, nachdem der Job abgeschlossen ist.

pre-snapshot

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, bevor der Snapshot erfasst wird.

post-snapshot

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, nachdem der Snapshot erfasst wird.

D2D_TARGETVOLUME

Identifiziert das Volume, das während eines Sicherungsjobs gesichert wird. Diese Variable ist anwendbar für Prä-/Post-Snapshot-Skripts für einen Sicherungsjob.

D2D_JOBRESULT

Identifiziert das Ergebnis für ein Post-Job-Skript. Die folgenden Werte identifizieren die D2D_JOBRESULT-Variable:

success

Identifiziert das Ergebnis als erfolgreich.

fail

Identifiziert das Ergebnis als nicht erfolgreich.

D2DSVR_HOME

Identifiziert den Ordner, in dem der Sicherungsserver installiert ist. Diese Variable ist anwendbar für die Skripts, die auf dem Sicherungsserver ausgeführt werden.

Das Skript ist erstellt.

Hinweis: Bei allen Skripten zeigt der Rückgabewert von Null eine erfolgreiche Erstellung an, und ein Rückgabewert, der ungleich Null ist, weist auf einen Fehler hin.

Überprüfung des Skripts in den Ordner "Prepost" und Überprüfung des Skripts

Alle Prä-/Post-Skripts für einen Sicherungsserver werden zentral vom Ordner "prepost" am folgenden Speicherort verwaltet:

```
/opt/CA/d2dserver/usr/prepost
```

Gehen Sie wie folgt vor:

1. Fügen Sie die Datei in folgenden Speicherort des Sicherungsservers ein:

   ```
   /opt/CA/d2dserver/usr/prepost
   ```

2. Geben Sie der Skriptdatei Ausführungsberechtigungen.
3. Melden Sie sich bei der Arcserve UDP Agent (Linux)-Webbenutzeroberfläche an.
4. Öffnen Sie den **Sicherungsassistenten** oder **Wiederherstellungsassistenten**, und navigieren Sie zur Registerkarte **Erweitert**.
5. Wählen Sie die Skriptdatei in der Drop-down-Liste **Einstellungen vor/nach dem Skript** aus, und übergeben Sie den Job.
6. Klicken Sie auf "**Aktivitätsprotokoll**", und stellen Sie sicher, dass das Skript für den angegebenen Sicherungsjob ausgeführt wird.

   Das Skript wird ausgeführt.

Die Prä-/Post-Skripte wurden erfolgreich erstellt und befinden sich im Ordner "prepost".

Erneutes Ausführen des Sicherungsjobs

Führen Sie den Sicherungsjob aus, sodass ein Wiederherstellungspunkt erstellt wird. Sie können diesen Wiederherstellungspunkt zur Datenwiederherstellung verwenden.

Überprüfen Sie auf der "Zusammenfassung" die Übersicht der Sicherungsdetails, und geben Sie einen Jobnamen an, um ihn von anderen Jobs zu unterscheiden.

Gehen Sie wie folgt vor:

1. Überprüfen Sie die Zusammenfassung, und geben Sie einen Jobnamen ein.

   Im Feld "Jobname" ist zunächst ein Standardname angegeben. Sie können einen neuen Jobnamen Ihrer Wahl eingeben, wobei das Feld jedoch nicht leer gelassen werden darf.

2. (Optional) Klicken Sie auf "Zurück", um die Einstellungen auf den Seiten des Assistenten zu ändern.
3. Klicken Sie auf "Übergeben".

   Der Sicherungsvorgang beginnt. Der Job wird der Registerkarte "Jobstatus" hinzugefügt, und der Sicherungsstatus wird angezeigt.

Der Sicherungsjob wird erstellt und ausgeführt.

Überprüfen, ob die Sicherung erfolgreich ausgeführt wurde

Nachdem der Sicherungsjob abgeschlossen ist, überprüfen Sie, dass der Wiederherstellungspunkt am angegebenen Ziel erstellt wurde.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu dem angegebenen Ziel, wo Sie Ihre Sicherungsdaten gespeichert haben.
2. Überprüfen Sie, dass die Sicherungsdaten in diesem Ziel vorhanden sind.

   Wenn der Name des Sicherungsjobs zum Beispiel "*Demo*" lautet und das Sicherungsziel xxx.xxx.xxx.xxx:/Data ist, dann navigieren Sie zum Sicherungsziel, und überprüfen Sie, dass ein neuer Wiederherstellungspunkt generiert wurde.

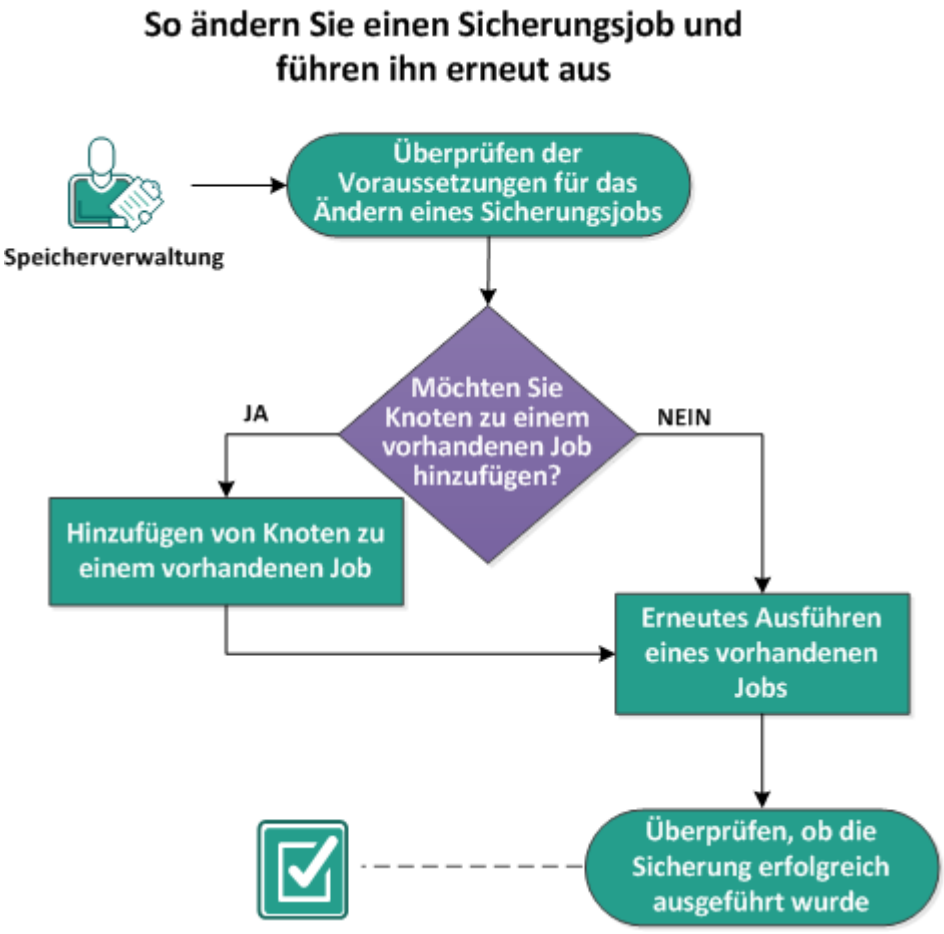
   Die Sicherungsdaten wurden erfolgreich überprüft.

Die Linux-Knoten wurden erfolgreich gesichert.

So ändern Sie einen Sicherungsjob und führen ihn erneut aus

Wenn Sie bereits einen Job für einen Knoten erstellt haben, können Sie ihn ändern und wiederholt ausführen. Sie müssen keinen weiteren Job erstellen, um den gleichen Knoten zu schützen. Wenn Sie keine Änderungen am Job vornehmen möchten, können Sie den Job auch ausführen, ohne ihn zu ändern. Einen Job zu ändern bedeutet, einen Knoten zu einem vorhandenen Job hinzuzufügen und/oder die Jobeinstellungen zu konfigurieren.

Die folgende Abbildung veranschaulicht den Vorgang zum Ändern und erneuten Ausführen eines Sicherungsjobs:


So ändern Sie einen Sicherungsjob und führen ihn erneut aus
Speicherverwaltung
Überprüfen der Voraussetzungen für das Ändern eines Sicherungsjobs
Möchten Sie Knoten zu einem vorhandenen Job hinzufügen?
JA
NEIN
Hinzufügen von Knoten zu einem vorhandenen Job
Erneutes Ausführen eines vorhandenen Jobs
Überprüfen, ob die Sicherung erfolgreich ausgeführt wurde

Führen Sie die folgenden Aufgaben aus, um einen Sicherungsjob zu ändern und neu auszuführen:

- Überprüfen der Voraussetzungen für das Ändern eines Sicherungsjobs (siehe Seite 78)
- Möchten Sie Knoten zu einem vorhandenen Job hinzufügen? (siehe Seite 78)
- Hinzufügen von Knoten zu einem vorhandenen Job (siehe Seite 78)
- Erneutes Ausführen eines vorhandenen Jobs (siehe Seite 79)
- Überprüfen, ob die Sicherung erfolgreich ausgeführt wurde (siehe Seite 80)

Überprüfen der Voraussetzungen für das Ändern eines Sicherungsjobs

Überprüfen Sie die folgenden Anforderungen, bevor Sie einen Sicherungsjob ändern und erneut ausführen:

- Es ist ein gültiger Sicherungsjob vorhanden.
- Sie haben die Knoten zu Arcserve UDP hinzugefügt.
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Möchten Sie Knoten zu einem vorhandenen Job hinzufügen?

Wenn bereits ein Sicherungsjob vorhanden ist und Sie neue Knoten mit denselben Sicherungseinstellungen schützen möchten, können Sie Knoten zu einem vorhandenen Job hinzufügen. Nachdem Sie die Knoten hinzugefügt haben, können Sie auch die Sicherungseinstellungen ändern und den Job ausführen.

Hinzufügen von Knoten zu einem vorhandenen Job

Sie können einem vorhandenen Sicherungsjob neue Knoten hinzufügen und den Job anschließend erneut ausführen. Alle Einstellungen des ausgewählten Jobs werden auf den neuen Knoten angewendet, und Sie müssen keine neuen Sicherungseinstellungen konfigurieren. Verwenden Sie diese Option, wenn Sie die gleichen Sicherungseinstellungen für alle Knoten verwenden möchten.

Gehen Sie wie folgt vor:

1. Wählen Sie im Statusfenster alle neuen Knoten auf der Registerkarte "Knoten" aus.
2. Klicken Sie im Menü "Assistent" auf "Sicherung", und wählen Sie "Ausgewählte Knoten zu einem vorhandenen Job hinzufügen".

   Das Dialogfeld "Ausgewählte Knoten zu einem vorhandenen Job hinzufügen" wird geöffnet.
3. Wählen Sie einen Job aus der Drop-down-Liste "Jobname" aus, und klicken Sie auf "OK".

   Der Knoten wird dem ausgewählten Sicherungsjob hinzugefügt, und die Spalte "Geschützt" auf der Registerkarte "Knoten" wird in "Ja" geändert.

Die Knoten werden zum vorhandenen Job hinzugefügt.

Erneutes Ausführen eines vorhandenen Sicherungsjobs

Führen Sie den Sicherungsjob erneut aus, um eine weitere Sicherung der angegebenen Knoten durchzuführen. Nach jeder erfolgreichen Sicherung wird ein Wiederherstellungspunkt erstellt. Wenn Sie einen Knoten bereits gesichert haben, müssen Sie keinen weiteren Sicherungsjob erstellen, um diesen Knoten erneut zu sichern. Alle früheren Jobs werden im Statusfenster auf der Registerkarte "Jobstatus" aufgeführt.

Wenn Sie einen Sicherungsjob erneut ausführen, geben Sie den Typ des Jobs an, den Sie durchführen möchten.

Hinweis: Wenn Sie Information auf der Seite "Sicherungsziel" des Sicherungsassistenten aktualisieren, bevor Sie einen Job erneut ausführen, ändert sich der Jobtyp automatisch in *Vollständige Sicherung*.

Gehen Sie wie folgt vor:

1. Geben Sie die URL von Arcserve UDP Agent (Linux) in einem Webbrowser ein, um die Benutzeroberfläche zu öffnen.

   Hinweis: Während der Installation von Arcserve UDP Agent (Linux) haben Sie die URL erhalten, um auf den Server zugreifen und ihn verwalten zu können.

2. Klicken Sie auf die Registerkarte "Jobstatus", und wählen Sie den Job aus, den Sie ausführen möchten.

3. Stellen Sie sicher, dass der Status des ausgewählten Jobs "Fertig" oder "Bereit" lautet.

   "Fertig" gibt an, dass der Job nicht geplant ist, und "Bereit" gibt an, dass der Job geplant ist.

4. Führen Sie einen der folgenden Schritte aus:

   - Um den Job ohne Änderungen auszuführen, gehen Sie wie folgt vor:

     a. Klicken Sie im Menü "Job" auf "Jetzt ausführen".

        Das Dialogfeld "Sicherungsjob jetzt ausführen" wird geöffnet.

     b. Wählen Sie den Sicherungstyp aus.

     c. Wählen Sie eine Option aus der Drop-down-Liste Job ausführen für aus:

        Ausgewählter Knoten

        Gibt an, dass der Sicherungsjob nur für den ausgewählten Knoten ausgeführt wird.

        Alle vom ausgewählten Job geschützten Knoten

        Gibt an, dass der Sicherungsjob für alle Knoten ausgeführt wird, die vom ausgewählten Job geschützt werden.

d. Klicken Sie auf "OK".

Das Dialogfeld "Sicherungsjob jetzt ausführen" wird geschlossen. Der Status des Jobs ändert auf der Registerkarte "Jobstatus" in "Aktiv", und der gleiche Job wird erneut ausgeführt.

- Um den Job vor dem Ausführen zu ändern, gehen Sie wie folgt vor:

  a. Wählen Sie einen Job aus, und klicken Sie auf "Ändern".

  Der Sicherungsassistent wird geöffnet.

  b. Aktualisieren Sie das erforderliche Feld im Sicherungsassistenten.

  c. Klicken Sie auf "Übergeben".

  Der Job wird je nach dem Ablaufplan für einen Job ausgeführt.

Der Sicherungsjob wird erfolgreich erneut ausgeführt.

Überprüfen, ob die Sicherung erfolgreich ausgeführt wurde

Nachdem der Sicherungsjob abgeschlossen ist, überprüfen Sie, dass der Wiederherstellungspunkt am angegebenen Ziel erstellt wurde.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu dem angegebenen Ziel, wo Sie Ihre Sicherungsdaten gespeichert haben.
2. Überprüfen Sie, dass die Sicherungsdaten in diesem Ziel vorhanden sind.

   Wenn der Name des Sicherungsjobs zum Beispiel "*Demo*" lautet und das Sicherungsziel xxx.xxx.xxx.xxx:/Data ist, dann navigieren Sie zum Sicherungsziel, und überprüfen Sie, dass ein neuer Wiederherstellungspunkt generiert wurde.

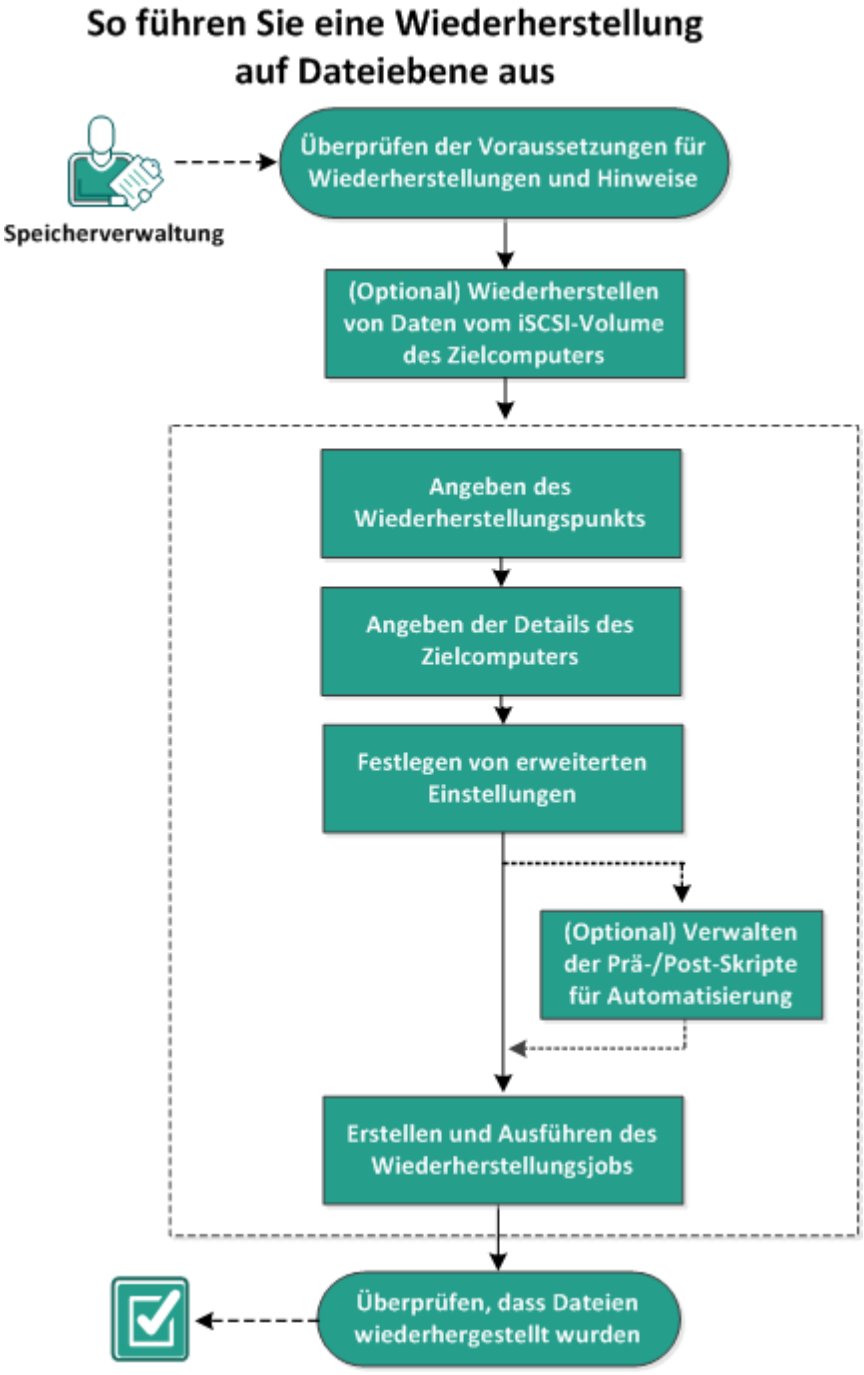
   Die Sicherungsdaten wurden erfolgreich überprüft.

Der Sicherungsjob wurde erfolgreich geändert und neu ausgeführt.

So führen Sie eine Wiederherstellung der Dateiebene unter Linux-Knoten aus

Bei einer Wiederherstellung auf Dateiebene werden einzelne Dateien und Verzeichnisse von einem Wiederherstellungspunkt aus wiederhergestellt. Sie können auch nur eine Datei von dem Wiederherstellungspunkt aus wiederherstellen. Diese Option ist hilfreich, wenn Sie nur ausgewählte Dateien und nicht den gesamten Wiederherstellungspunkt wiederherstellen möchten.

Folgendes Diagramm zeigt den Prozess an, um eine Wiederherstellung der Dateiebene auszuführen:


So führen Sie eine Wiederherstellung auf Dateiebene aus
Speicherverwaltung
Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise
(Optional) Wiederherstellen von Daten vom iSCSI-Volume des Zielcomputers
Angeben des Wiederherstellungspunkts
Angeben der Details des Zielcomputers
Festlegen von erweiterten Einstellungen
(Optional) Verwalten der Prä-/Post-Skripte für Automatisierung
Erstellen und Ausführen des Wiederherstellungsjobs
Überprüfen, dass Dateien wiederhergestellt wurden

Gehen Sie zum Ausführen einer Wiederherstellung auf Dateiebene wie folgt vor:

- Überprüfen der Voraussetzungen für die Wiederherstellung (siehe Seite 82)
- (Optional) Wiederherstellen von Daten des iSCSI-Volume des Zielcomputers (siehe Seite 83)
- Angeben des Wiederherstellungspunkts (siehe Seite 84)
- Angeben der Details des Zielcomputers (siehe Seite 88)
- Festlegen von erweiterten Einstellungen (siehe Seite 92)
- (Optional) Verwalten der Prä-/Post-Skripte für Automatisierung (siehe Seite 93)
- Erstellen und Ausführen des Wiederherstellungsjobs (siehe Seite 96)
- Überprüfen, dass Dateien wiederhergestellt wurden (siehe Seite 97)

Überprüfen der Voraussetzungen

Beachten Sie Folgendes, bevor Sie eine Wiederherstellung auf Dateiebene ausführen:

- Sie verfügen über einen gültigen Wiederherstellungspunkt und, falls erforderlich, über das Verschlüsselungskennwort.
- Sie verfügen über einen gültigen Zielknoten zum Wiederherstellen der Daten.
- Sie haben sichergestellt, dass der Linux-Sicherungsserver das Dateisystem unterstützt, das Sie wiederherstellen möchten.

  RedHat 5.x unterstützt zum Beispiel nicht das Dateisystem *reiserfs*. Wenn das Betriebssystem des Sicherungsservers RedHat 5.x ist und Sie das Dateisystem "reiserfs" wiederherstellen möchten, müssen Sie den Dateisystemtreiber installieren, um "reiserfs" zu unterstützen. Sie können Arcserve UDP Agent (Linux)-Live-CD auch verwenden, um die Wiederherstellung auf Dateiebene auszuführen, da Live-CD alle Dateisystemtypen unterstützt.
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

(Optional) Wiederherstellen von Daten des iSCSI-Volume des Zielcomputers

Wenn Sie Ihre Daten auf einem iSCSI-Zieldatenträger gespeichert haben, können Sie eine Verbindung mit dem iSCSI-Volume herstellen und Daten wiederherstellen. Das iSCSI-Volume ermöglicht das Verwalten und Übertragen von Daten über ein Netzwerk.

Stellen Sie sicher, dass Sie die neueste Version der iSCSI-Initiator-Software auf Ihrem Sicherungsserver installiert haben. In RHEL-Systemen ist die Initiator-Software als "iscsi-initiator-utils" gepackt. In SLES-Systemen ist die Initiator-Software als "open-iscsi" gepackt.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Shell-Umgebung des Sicherungsservers an.
2. Führen Sie einen der folgenden Befehle aus, um den iSCSI-Initiator-Daemon zu starten.
   - Für RHEL-Systeme:

     ```
     /etc/init.d/iscsid start
     ```

     In RHEL-Systemen heißt der Dienst "iscsid".
   - Für SLES-Systeme:

     ```
     /etc/init.d/open-iscsi start
     ```

     In SLES-Systemen heißt der Dienst "open-iscsi".
3. Führen Sie ein Discovery-Skript aus, um den iSCSI-Zielhost zu erkennen.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADRESSE>:<Portnummer>
   ```

   Der Standardportwert des iSCSI-Zielhost ist 3260.
4. Notieren Sie den iSCSI Qualified Name (IQN) des iSCSI-Zielhost, der durch das Discovery-Skript gefunden wird, bevor Sie sich manuell beim erkannten Zielcomputer anmelden.
5. Listen Sie das verfügbare Blockgerät des Sicherungsservers auf.

   ```
   #fdisk -l
   ```
6. Melden Sie sich beim erkannten Ziel an.

   ```
   iscsiadm -m node -T <iSCSI Target IQN name> -p
   <ISCSI-SERVER-IP-ADRESSE>:<Portnummer>  -l
   ```

   Im Verzeichnis /dev des Sicherungsservers wird ein Blockgerät angezeigt.

7. Führen Sie den folgenden Befehl aus, um den Namen des neuen Geräts abzurufen:

   ```
   #fdisk –l
   ```

   Im Sicherungsserver können Sie ein zusätzliches Gerät, /dev/sd<x>, sehen.

   In diesem Beispiel ist der Name des Geräts "/dev/sdc". In den folgenden Schritten wird dieser Gerätename verwendet, um eine Partition und ein Dateisystem zu erstellen.

8. Laden Sie das iSCSI-Volume mithilfe der folgenden Befehle:

   ```
   # mkdir /iscsi
   ```

   ```
   # mount /dev/sdc1 /iscsi
   ```

   Hinweis: Wenn Sie den Sitzungsspeicherort im Wiederherstellungsassistenten angeben, müssen Sie "Lokal" auswählen und den Pfad /iscsi eingeben.

   Beispiel: <Pfad>/iscsi

9. (Optional) Fügen Sie folgenden Datensatz zur Datei "/etc/fstab" hinzu, damit das iSCSI-Volume automatisch eine Verbindung zum Sicherungsserver herstellt, nachdem Sie den Server neu gestartet haben.

   ```
   /dev/sdc1 /iscsi ext3 _netdev 0 0
   ```

Der Sicherungsserver kann jetzt eine Verbindung mit dem iSCSI-Volume herstellen und Daten vom iSCSI-Volume wiederherstellen.

Angeben des Wiederherstellungspunkts

Bei jedem Ausführen einer Sicherung wird ein Wiederherstellungspunkt erstellt. Geben Sie die Informationen zu den Wiederherstellungspunkten im **Wiederherstellungsassistenten** an, damit genau die gewünschten Daten wiederhergestellt werden. Sie können je nach Bedarf bestimmte Dateien oder alle Dateien wiederherstellen.

Hinweis: Wenn Sie "**Quelle - lokal**" als Sicherungsziel ausgewählt haben, kann der Sicherungsserver keine direkte Verbindung mit der lokalen Quelle herstellen. Um auf die lokale Quelle zuzugreifen, müssen Sie zusätzliche Konfigurationen durchführen.

Gehen Sie wie folgt vor, um Dateien über "Quelle - lokal" wiederherzustellen:

a. Geben Sie das Sicherungsziel (Quelle - lokal) frei, und stellen Sie sicher, dass der Sicherungsserver eine Verbindung zum Sicherungsziel herstellen kann.

b. Fügen Sie dem Sicherungsserver das freigegebene Ziel als Sicherungsspeicherort hinzu.

"Quelle - lokal" verhält sich jetzt wie ein NFS-Sicherungsspeicherort, und Sie können Dateien der Freigabe wiederherstellen.

Gehen Sie wie folgt vor:

1. Führen Sie einen der folgenden Vorgänge durch, um auf den Wiederherstellungs-Assistenten zuzugreifen:
   - In Arcserve UDP:
     a. Melden Sie sich bei Arcserve UDP an.
     b. Klicken Sie auf die Registerkarte **Ressourcen**.
     c. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

        Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.
     d. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Aktionen**.
     e. Klicken Sie im Drop-down-Menü **Aktionen** auf **Wiederherstellen**.

        Die Arcserve UDP Agent (Linux)-Webbenutzeroberfläche wird geöffnet. Das Auswahldialogfeld für den Wiederherstellungstyp wird in der Benutzeroberfläche des Agenten angezeigt.
     f. Wählen Sie den Wiederherstellungstyp aus, und klicken Sie auf **OK**.

        Hinweis: Sie werden automatisch beim Agentenknoten angemeldet, und der **Wiederherstellungsassistent** wird im Agentenknoten geöffnet.

- In Arcserve UDP Agent (Linux):
  a. Öffnen Sie die Arcserve UDP Agent (Linux)-Webbenutzeroberfläche.

     Hinweis: Während der Installation von Arcserve UDP Agent (Linux) haben Sie die URL erhalten, um auf den Server zugreifen und ihn verwalten zu können. Melden Sie sich bei Arcserve UDP Agent (Linux) an.

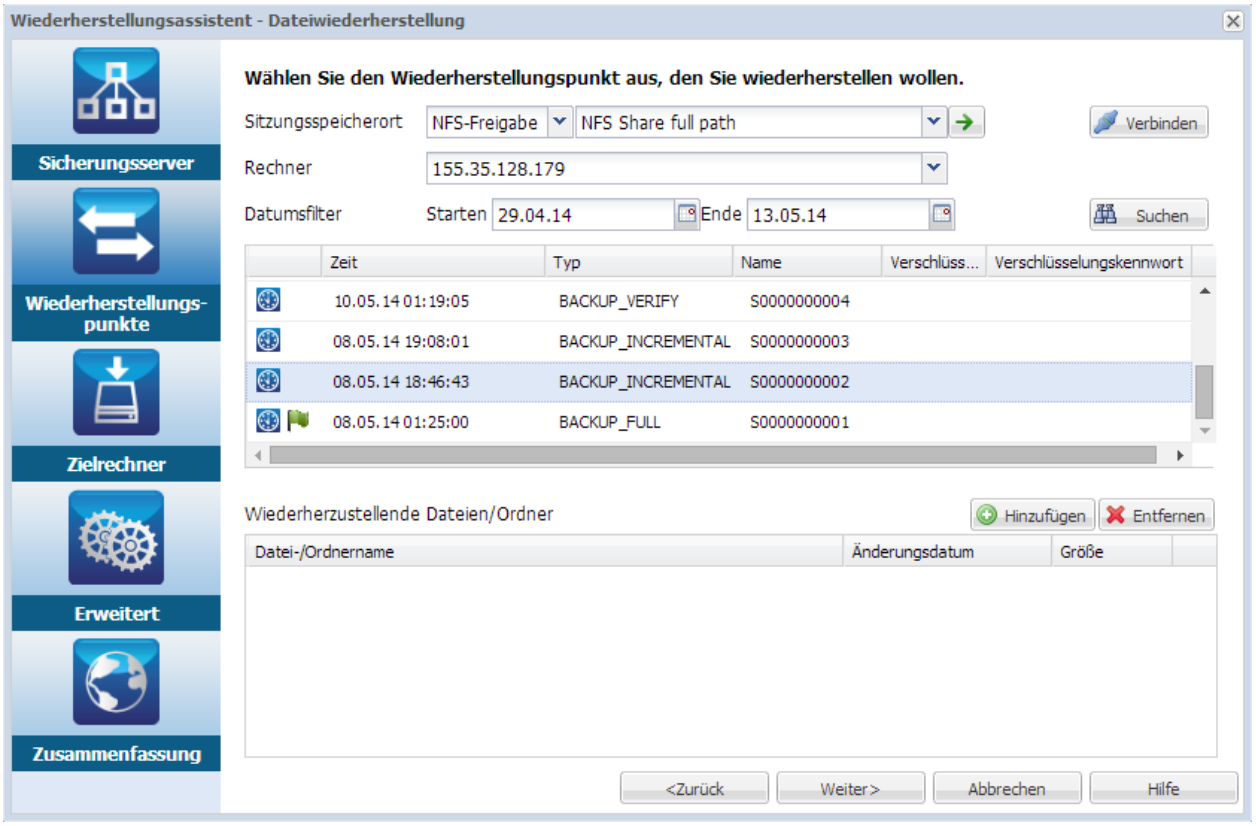
  b. Klicken Sie im Menü "**Assistent**" auf "**Wiederherstellen**", und wählen Sie "**Wiederherstellungsdatei**".

     Wiederherstellungs-Assistent - Datei-Wiederherstellung wird geöffnet.

Der ausgewählte Sicherungsserver wird auf der Seite **Sicherungsserver** des **Wiederherstellungsassistenten** angezeigt. Sie können in der Drop-down-Liste **Sicherungsserver** keine Optionen auswählen.

2. Klicken Sie auf "**Weiter**".

   Die Seite **Wiederherstellungspunkte** des **Wiederherstellungsassistenten** wird geöffnet. Der letzte Wiederherstellungspunkt ist ausgewählt.



3. Wählen Sie eine Sitzung aus der Drop-down-Liste "**Sitzungsspeicherort**" aus, wenn Sie eine andere Sitzung wiederherstellen möchten, und geben Sie den vollständigen Pfad der Freigabe an.

   Nehmen Sie zum Beispiel an, dass der Sitzungsspeicherort eine NFS-Freigabe, xxx.xxx.xxx.xxx die IP-Adresse der NFS-Freigabe und der Ordnernamen "*Daten*" ist. Sie geben dann "xxx.xxx.xxx.xxx:/Data" als Speicherort der NFS-Freigabe an.

   Hinweis: Wenn die gesicherten Daten unter "Quelle - lokal" gespeichert werden, müssen Sie den Quellknoten zuerst in einen NFS-Server konvertieren und dann den Sitzungsspeicherort freigeben.

4. Klicken Sie auf "**Verbinden**".

   Alle Knoten, die an diesem Speicherort gesichert wurden, werden in der Drop-down-Liste "**Rechner**" aufgelistet.

5. Wählen Sie den Knoten, von dem Sie eine Wiederherstellung vornehmen möchten, in der Drop-down-Liste "**Rechner**" aus.

   Es werden alle Wiederherstellungspunkte des ausgewählten Knotens aufgelistet.

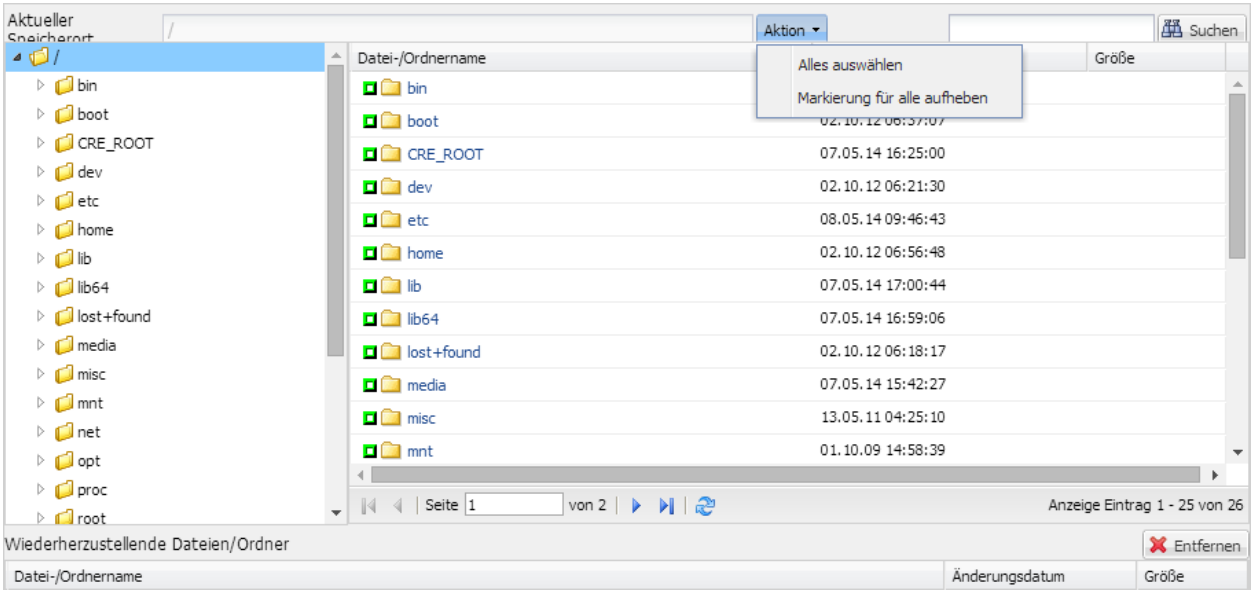
6. Wenden Sie den Datumsfilter an, um die Wiederherstellungspunkte anzuzeigen, die zwischen dem angegebenen Datum generiert werden, und klicken Sie auf **Suchen**.

   Standard: Die letzten zwei Wochen.

   Alle verfügbaren Wiederherstellungspunkte zwischen den angegebenen Datumswerten werden angezeigt.

7. Wählen Sie den gewünschten Wiederherstellungspunkt aus, und klicken Sie auf "**Hinzufügen**". Wenn der Wiederherstellungspunkt verschlüsselt ist, geben Sie das Verschlüsselungskennwort ein, um die Daten wiederherzustellen.

   Das Dialogfeld **<Knotenname> durchsuchen** wird geöffnet.



8. Wählen Sie die Dateien und Ordner aus, die Sie wiederherstellen möchten, und klicken Sie auf "**OK**".

   Hinweis: Wenn Sie versuchen, eine Datei oder einen Ordner mithilfe des **Suchfeldes** zu finden, stellen Sie sicher, dass Sie den höchsten Ordner in der Hierarchie auswählen. Die Suche wird in allen untergeordneten Ordnern des ausgewählten Ordners durchgeführt.

   Das Dialogfeld **<Knotenname> durchsuchen** wird geschlossen, und Sie gelangen erneut zur Seite **Wiederherstellungspunkte**. Die ausgewählten Dateien und Ordner sind unter" **Wiederherzustellende Dateien/Ordner**" aufgeführt.

9. Klicken Sie auf "**Weiter**".

   Die Seite "**Zielcomputer**" wird geöffnet.

Der Wiederherstellungspunkt wird angegeben.

Angeben der Details des Zielcomputers

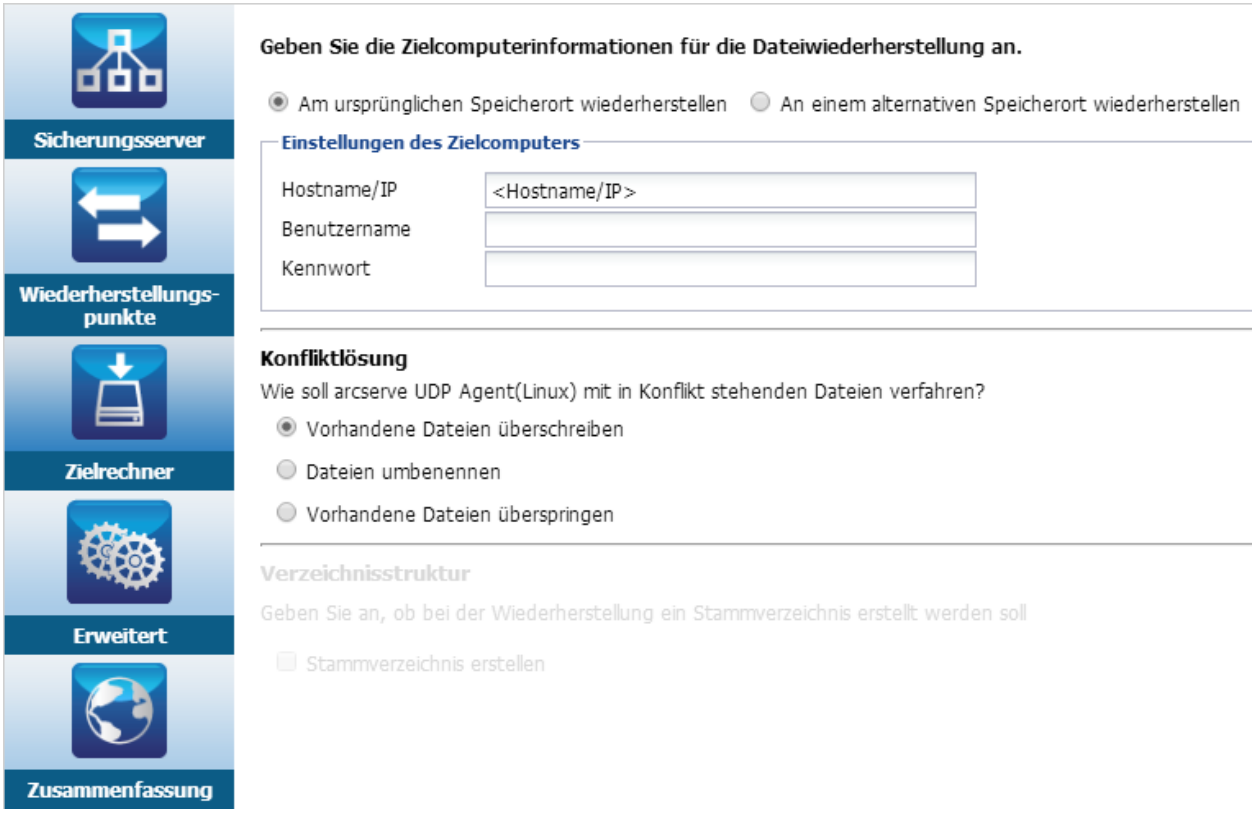
Geben Sie die Details des Zielknotens an, damit Daten auf diesem Knoten wiederhergestellt werden. Sie können die ausgewählten Dateien oder Ordner auf dem Quellknoten oder einem neuen Knoten wiederherstellen.

Gehen Sie wie folgt vor:

- Gehen Sie wie folgt vor, um die Daten auf dem Knoten wiederherzustellen, von dem sie gesichert wurden:

  1. Wählen Sie auf der Seite "**Zielcomputer**" die Option "**Am ursprünglichen Speicherort wiederherstellen**".

     Das Feld "**Hostname**" unter "**Einstellungen des Zielcomputers**" wird mit dem Namen des Quellknotens ausgefüllt.



2. Geben Sie den Benutzernamen und das Kennwort des Knotens ein.
3. Wählen Sie eine der folgenden Optionen, um Dateikonflikte zu lösen:

   Vorhandene Dateien überschreiben

   Gibt an, dass die Sicherungsdatei vom Wiederherstellungspunkt die vorhandene Datei ersetzt, wenn die Datei auf dem Zielcomputer vorhanden ist.

   Dateien umbenennen

   Gibt an, dass, wenn die Datei im Zielcomputer vorhanden ist, eine neue Datei mit dem gleichen Dateinamen und der Dateierweiterung *.d2dduplicate<x>* erstellt wird. <x> gibt an, wie oft die Datei wiederhergestellt wird. Alle Daten werden dann in eine neue Datei wiederhergestellt.

   Vorhandene Dateien überspringen

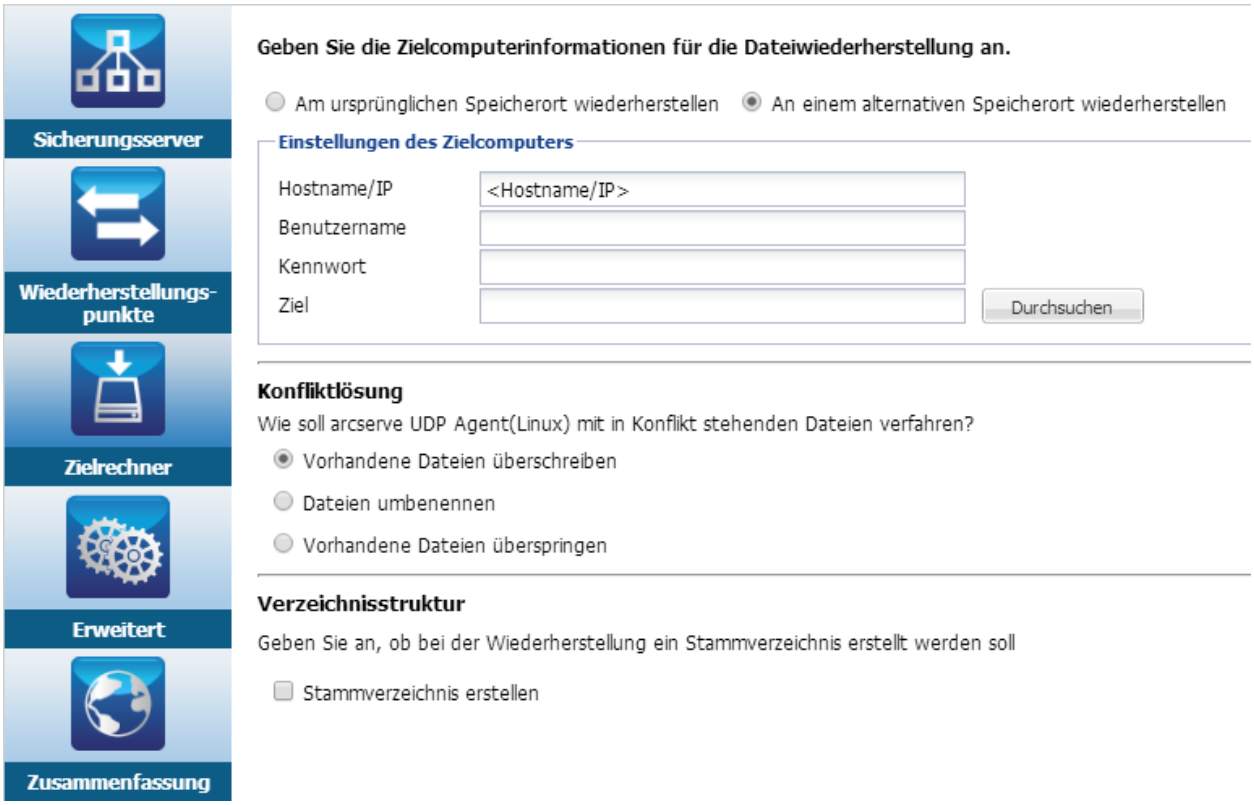
   Gibt an, dass die Dateien, wenn die gleiche Datei auf dem Zielcomputer vorhanden ist, nicht vom Wiederherstellungspunkt wiederhergestellt werden.

4. Klicken Sie auf "**Weiter**".

   Das Dialogfeld **"Erweitert"** wird geöffnet.

- Gehen Sie wie folgt vor, um die Wiederherstellung auf einen neuen Knoten durchzuführen:

  1. Wählen Sie auf der Seite "**Zielcomputer**" die Option "**An einem alternativen Speicherort wiederherstellen**".



  2. Geben Sie den Hostnamen oder die IP-Adresse des Zielknotens ein.
  3. Geben Sie den Benutzernamen und das Kennwort des Knotens ein.
  4. Geben Sie den Pfad ein, in dem die Daten wiederhergestellt werden sollen, oder klicken Sie auf "**Durchsuchen**", um den Ordner auszuwählen, in dem die Daten wiederhergestellt werden sollen, und klicken Sie dann auf "**OK**".

5. Wählen Sie eine der folgenden Optionen, um Dateikonflikte zu lösen:

   Vorhandene Dateien überschreiben

   Gibt an, dass die Sicherungsdatei vom Wiederherstellungspunkt die vorhandene Datei ersetzt, wenn die Datei auf dem Zielcomputer vorhanden ist.

   Dateien umbenennen

   Gibt an, dass, wenn die Datei im Zielcomputer vorhanden ist, eine neue Datei mit dem gleichen Dateinamen und der Dateierweiterung *.d2dduplicate<x>* erstellt wird. <x> gibt an, wie oft die Datei wiederhergestellt wird. Alle Daten werden dann in eine neue Datei wiederhergestellt.

   Vorhandene Dateien überspringen

   Gibt an, dass die Dateien, wenn die gleiche Datei auf dem Zielcomputer vorhanden ist, nicht vom Wiederherstellungspunkt wiederhergestellt werden.

6. (Optional) Wählen Sie "**Stammverzeichnis erstellen**".
7. Klicken Sie auf "**Weiter**".

Das Dialogfeld **"Erweitert"** wird geöffnet.

Die Details des Zielcomputers sind angegeben.

Festlegen von erweiterten Einstellungen

Geben Sie die erweiterten Einstellungen an, um eine geplante Wiederherstellung der Daten auszuführen. Mit einer geplanten Wiederherstellung wird sichergestellt, dass die Daten auch bei Ihrer Abwesenheit zur angegebenen Zeit wiederhergestellt werden.

Gehen Sie wie folgt vor:

1. Legen Sie Datum und Uhrzeit für den Beginn fest, indem Sie eine der folgenden Optionen auswählen:

   Jetzt ausführen

   Startet den Wiederherstellungsjob auf Dateiebene sofort, nachdem Sie den Job übergeben haben.

   Startdatum und -zeitpunkt festlegen

   Startet den Wiederherstellungsjob auf Dateiebene zum angegebenen Datum und Zeitpunkt, nachdem Sie den Job übergeben haben.

2. (Optional) Wählen Sie "**Geschätzte Dateigröße**".
3. (Optional) Wählen Sie ein Skript aus der Option **Einstellungen für Prä-/Post-Skripts** aus.

   Diese Skripte führen Skriptbefehle für Aktionen aus, die vor dem Start des Jobs und/oder nach Abschluss des Jobs durchgeführt werden sollen.

   Hinweis: Die Felder für **Einstellungen vor/nach dem Skript** werden nur aufgefüllt, wenn Sie bereits eine Skriptdatei erstellt und an folgendem Speicherort platziert haben:

   ```
   /opt/CA/d2dserver/usr/prepost
   ```

   Hinweis: Weitere Informationen zur Erstellung der Prä-/Post-Skripte finden Sie unter *Verwalten der Prä-/Post-Skripte für Automatisierung* (siehe Seite 156).
4. Klicken Sie auf "**Weiter**".

   Die Seite **"Zusammenfassung"** wird geöffnet.

Die erweiterten Einstellungen sind angegeben.

(Optional) Verwalten der Prä-/Post-Skripte für Automatisierung

Mit Prä-/Post-Skripts können Sie Ihre eigene Geschäftslogik in bestimmten Phasen eines in Bearbeitung befindlichen Jobs ausführen. Sie können in **Einstellungen vor/nach dem Skript** des **Sicherungsassistenten** und des **Wiederherstellungsassistenten** auf der Benutzeroberfläche angeben, wann Ihre Skripte ausgeführt werden sollen. Die Skripts können je nach Einstellung auf dem Sicherungsserver ausgeführt werden.

Das Verwalten von Prä-/Post-Skripts ist ein zweiteiliger Vorgang, der das Erstellen des Prä-/Post-Skripts und das Einfügen des Skripts in den "prepost"-Ordners umfasst.

Erstellen von Prä-/Post-Skripts

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Erstellen Sie eine Skriptdatei, indem Sie die Umgebungsvariablen in Ihrer bevorzugten Skripterstellungssprache verwenden.

   Umgebungsvariablen des Prä-/Post-Skripts

   Verwenden Sie die folgenden Umgebungsvariablen, um Ihr Skript zu erstellen:

   D2D_JOBNAME

   Gibt den Namen des Jobs an.

D2D_JOBID

Gibt die Job-ID an. Die Job-ID ist eine Nummer, die für den Job vergeben wird, wenn Sie den Job ausführen. Wenn Sie den gleichen Job erneut ausführen, erhalten Sie eine neue Jobnummer.

D2D_TARGETNODE

Identifiziert den Knoten, der gesichert oder wiederhergestellt wird.

D2D_JOBTYPE

Identifiziert den Typ des ausgeführten Jobs. Die folgenden Werte identifizieren die D2D_JOBTYPE-Variable:

backup.full

Identifiziert den Job als eine vollständige Sicherung.

backup.incremental

Identifiziert den Job als eine Zuwachssicherung.

backup.verify

Identifiziert den Job als eine Überprüfungssicherung.

restore.bmr

Identifiziert den Job als eine Bare-Metal-Recovery (BMR). Dies ist ein Wiederherstellungsjob.

restore.file

Identifiziert den Job als eine Wiederherstellung auf Dateiebene. Dies ist ein Wiederherstellungsjob.

D2D_SESSIONLOCATION

Identifiziert den Speicherort, an dem die Wiederherstellungspunkte gespeichert sind.

D2D_PREPOST_OUTPUT

Identifiziert eine Temp-Datei. Der Inhalt der Anfangszeile der Temp-Datei wird im Aktivitätsprotokoll angezeigt.

D2D_JOBSTAGE

Gibt die Phase des Jobs an. Die folgenden Werte identifizieren die D2D_JOBSTAGE-Variable:

pre-job-server

Identifiziert das Skript, das auf dem Sicherungsserver ausgeführt wird, bevor der Job startet.

post-job-server

Identifiziert das Skript, das auf dem Sicherungsserver ausgeführt wird, nachdem der Job abgeschlossen ist.

pre-job-target

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, bevor der Job startet.

post-job-target

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, nachdem der Job abgeschlossen ist.

pre-snapshot

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, bevor der Snapshot erfasst wird.

post-snapshot

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, nachdem der Snapshot erfasst wird.

D2D_TARGETVOLUME

Identifiziert das Volume, das während eines Sicherungsjobs gesichert wird. Diese Variable ist anwendbar für Prä-/Post-Snapshot-Skripts für einen Sicherungsjob.

D2D_JOBRESULT

Identifiziert das Ergebnis für ein Post-Job-Skript. Die folgenden Werte identifizieren die D2D_JOBRESULT-Variable:

success

Identifiziert das Ergebnis als erfolgreich.

fail

Identifiziert das Ergebnis als nicht erfolgreich.

D2DSVR_HOME

Identifiziert den Ordner, in dem der Sicherungsserver installiert ist. Diese Variable ist anwendbar für die Skripts, die auf dem Sicherungsserver ausgeführt werden.

Das Skript ist erstellt.

Hinweis: Bei allen Skripten zeigt der Rückgabewert von Null eine erfolgreiche Erstellung an, und ein Rückgabewert, der ungleich Null ist, weist auf einen Fehler hin.

Überprüfung des Skripts in den Ordner "Prepost" und Überprüfung des Skripts

Alle Prä-/Post-Skripts für einen Sicherungsserver werden zentral vom Ordner "prepost" am folgenden Speicherort verwaltet:

```
/opt/CA/d2dserver/usr/prepost
```

Gehen Sie wie folgt vor:

1. Fügen Sie die Datei in folgenden Speicherort des Sicherungsservers ein:

   ```
   /opt/CA/d2dserver/usr/prepost
   ```

2. Geben Sie der Skriptdatei Ausführungsberechtigungen.
3. Melden Sie sich bei der Arcserve UDP Agent (Linux)-Webbenutzeroberfläche an.
4. Öffnen Sie den **Sicherungsassistenten** oder **Wiederherstellungsassistenten**, und navigieren Sie zur Registerkarte **Erweitert**.
5. Wählen Sie die Skriptdatei in der Drop-down-Liste **Einstellungen vor/nach dem Skript** aus, und übergeben Sie den Job.
6. Klicken Sie auf "**Aktivitätsprotokoll**", und stellen Sie sicher, dass das Skript für den angegebenen Sicherungsjob ausgeführt wird.

   Das Skript wird ausgeführt.

Die Prä-/Post-Skripte wurden erfolgreich erstellt und befinden sich im Ordner "prepost".

Erstellen und Ausführen des Wiederherstellungsjobs

Erstellen Sie den Wiederherstellungsjob, und führen Sie ihn aus, sodass Sie die Wiederherstellung auf Dateiebene initiieren können. Überprüfen Sie die Wiederherstellungspunktinformationen, bevor Sie die Dateien wiederherstellen. Bei Bedarf können Sie zurückgehen und die Wiederherstellungseinstellungen im Assistenten ändern.

Gehen Sie wie folgt vor:

1. Überprüfen Sie die Wiederherstellungsdetails auf der Seite **Zusammenfassung** des **Wiederherstellungsassistenten**.
2. (Optional) Klicken Sie auf **Zurück**, um Informationen zu ändern, die Sie auf den Seiten des **Wiederherstellungsassistenten** eingegeben haben.

3. Geben Sie einen Jobnamen ein, und klicken Sie auf "**Übergeben**".

   Im Feld "**Jobname**" ist zunächst ein Standardname angegeben. Sie können einen neuen Jobnamen Ihrer Wahl eingeben, wobei das Feld jedoch nicht leer gelassen werden darf.

   Der **Wiederherstellungsassistent** wird geschlossen. Der Status des Jobs wird auf der Registerkarte "**Jobstatus**" angezeigt.

Der Wiederherstellungsjob wurde erfolgreich erstellt und ausgeführt.

Überprüfen, dass Dateien wiederhergestellt wurden

Überprüfen Sie nach Abschluss des Wiederherstellungsjobs, dass alle Dateien im Zielknoten wiederhergestellt wurden. Überprüfen Sie die Registerkarten **Jobübersicht** und **Aktivitätsprotokoll** im Fenster **Status**, um den Fortschritt des Wiederherstellungsprozesses zu überwachen.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu dem Zielcomputer, auf dem Sie die Daten wiederhergestellt haben.
2. Überprüfen Sie, dass die erforderlichen Daten vom Wiederherstellungspunkt wiederhergestellt wurden.

   Die Dateien wurden erfolgreich überprüft.

Die Wiederherstellung auf Dateiebene wurde erfolgreich ausgeführt.

So erstellen Sie eine startfähige Live-CD

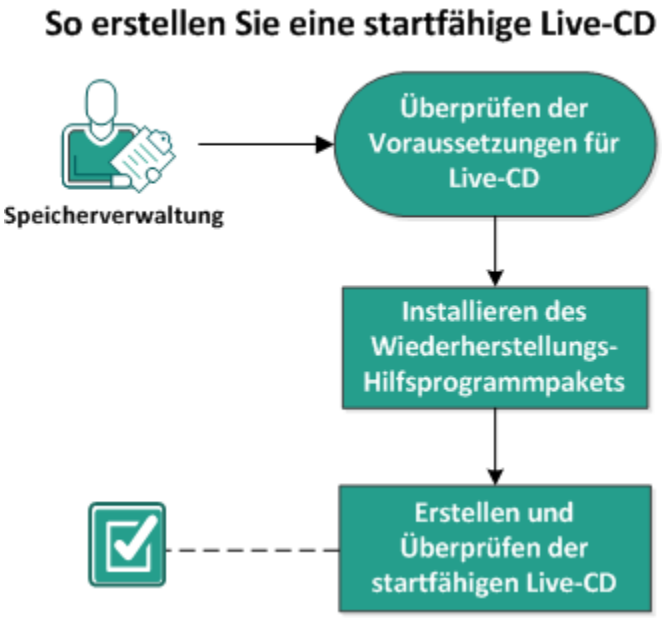
Als Storage Manager können Sie eine startfähige Live-CD erstellen. Wenn diese startfähige Live-CD erstellt ist, enthält sie ein vollständiges schreibgeschütztes Image des Computerbetriebssystems, und die Live-CD kann verwendet werden, um temporäre Betriebssystemfunktionen anzugeben. Diese Live-CD enthält Ihre gesamten Systemeinstellungen und Betriebssystemdateien und kann verwendet werden, um folgende Funktionen auszuführen:

- Sie können Arcserve UDP Agent (Linux) verwenden, ohne das Produkt tatsächlich zu installieren. Dies ermöglicht es Ihnen, das Produkt zu nutzen und auszuwerten, ohne es zu installieren oder Änderungen an der vorhandenen Festplatte Ihres Computers durchzuführen.
- Sie können Arcserve UDP Agent (Linux) (auf mehreren Servern) mithilfe von nur einem Setup-Paket installieren. Ohne Live-CD müssen Sie zwei separate Dateien installieren (die .bin-Datei und das Paket mit dem Wiederherstellungshilfsprogramm), um Arcserve UDP Agent (Linux) zu installieren. Das Wiederherstellungs-Hilfsprogrammpaket ist im gleichen Live-CD-Setup-Paket enthalten.
- Sie können eine Bare-Metal-Recovery (BMR) ausführen. Sie können diese Live-CD verwenden, um die IP-Adresse des Zielcomputers (der während der BMR erforderlich ist) abzurufen.

Der Ordner "bin" enthält die Skripte, die Sie von der Befehlszeile ausführen können, um eine startfähige Live-CD zu erstellen. Der Ordner "bin" befindet sich im folgenden Pfad:

```
# /opt/CA/d2dserver/bin
```

Folgendes Diagramm zeigt den Vorgang zur Erstellung einer startfähigen Live-CD:


So erstellen Sie eine startfähige Live-CD
Speicherverwaltung
Überprüfen der Voraussetzungen für Live-CD
Installieren des Wiederherstellungs-Hilfsprogrammpakets
Erstellen und Überprüfen der startfähigen Live-CD

In der folgenden Liste sind die Aufgaben aufgeführt, die zum Erstellen einer startfähigen Live-CD durchgeführt werden müssen:

- Überprüfen der Voraussetzungen für Live-CD (siehe Seite 99)
- Installieren des Wiederherstellungs-Hilfsprogrammpakets (siehe Seite 100)
- Erstellen und Überprüfen der startfähigen Live-CD (siehe Seite 100)

Überprüfen der Voraussetzungen für Live-CD

Beachten Sie die folgenden Voraussetzungen, bevor Sie eine Live-CD erstellen:

- Sie verfügen über die root-Anmeldeinformationen für die Anmeldung beim Sicherungsserver.
- Sie haben die Versionshinweise gelesen und kennen die Funktionen einer Live-CD.
- Sie verfügen über Kenntnisse hinsichtlich der Linux-Skripterstellung.
- Sie haben das *mkisofs-Tool* auf dem Sicherungsserver installiert. Der Sicherungsserver verwendet das mkisofs-Tool, um die Datei "Live CD.iso" zu erstellen.
- Sie haben mindestens 1.024 MB freien Speicher auf Ihrem Rechner, um die Live-CD zu starten und auszuführen.
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Installieren des Wiederherstellungs-Hilfsprogrammpakets

Sie müssen das Wiederherstellungs-Hilfsprogrammpaket installieren, um Wiederherstellungsvorgänge ausführen zu können. Wenn Sie das Wiederherstellungs-Hilfsprogrammpaket nicht installieren, können Sie keine Wiederherstellung auf Dateiebene oder BMR ausführen. Sie können das Wiederherstellungs-Hilfsprogrammpaket während der Installation von Arcserve UDP Agent (Linux) installieren. Sie können das Wiederherstellungs-Hilfsprogrammpaket auch herunterladen und jederzeit nach der Installation von Arcserve UDP Agent (Linux) installieren.

Nachdem Sie das Wiederherstellungs-Hilfsprogrammpaket installiert haben, können Sie eine Live-CD erstellen.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Navigieren Sie mit dem folgenden Befehl zum Ordner "bin":

   ```
   # cd /opt/CA/d2dserver/bin
   ```

3. Führen Sie den folgenden Befehl aus, um das Wiederherstellungs-Hilfsprogrammpaket zu installieren:

   ```
   # ./configutility
   ```

   Eine Meldung wird angezeigt, die Sie dazu auffordert, den Pfad des Wiederherstellungs-Hilfsprogrammpakets anzugeben.

4. Geben Sie den vollständigen Pfad an, wo Sie das Wiederherstellungs-Hilfsprogrammpaket heruntergeladen haben.

   Die Installation wird gestartet.

Das Wiederherstellungs-Hilfsprogrammpaket wird installiert.

Erstellen und Überprüfen der startfähigen Live-CD

Live-CD erstellt die Umgebung des Linux-Sicherungsservers, ohne die Software zu installieren. Live-CD vereinfacht die BMR anhand einer IP in einem privaten Netzwerk.

Live-CD ist ein vollständig startfähiges Computerbetriebssystem, das im Speicher des Computers ausgeführt und nicht von der Festplatte geladen wird. Live-CD ermöglicht es Ihnen, ein Betriebssystem zu testen und auszuwerten, ohne es installieren zu müssen oder das vorhandene Betriebssystem auf dem Computer zu ändern.

Gehen Sie wie folgt vor:

1. Navigieren Sie mit dem folgenden Befehl zum Ordner "bin":

   ```
   # cd /opt/CA/d2dserver/bin
   ```

2. Führen Sie folgenden Befehl aus, um eine Live-CD zu erstellen:

   ```
   # ./makelivecd
   ```

3. Navigieren Sie zum folgenden Speicherort, und überprüfen Sie, ob die Datei "LiveCD.iso" erstellt wurde:

   /opt/CA/d2dserver/packages

Sie haben die startfähige Live-CD erfolgreich erstellt und überprüft. Wenn Sie die Live-CD in einem virtuellen Netzwerk verwenden möchten, können Sie die Datei "LiveCD.iso" direkt auf den virtuellen Rechner laden. Wenn Sie die Live-CD auf einem physischen Rechner verwenden möchten, dann müssen Sie das LiveCD.iso-Image auf eine Mediendatei (CD oder DVD) brennen, und anschließend müssen Sie die Mediendatei verwenden, um Ihren Rechner zu starten.

So erstellen Sie eine CentOS-basierte Live-CD

Als Storage Manager können Sie eine startfähige CentOS-basierte Live-CD erstellen. Eine CentOS-Live-CD ist eine auf CentOS basierte Datenverarbeitungsumgebung innerhalb des Arbeitsspeichers. Der Zweck dieser Live-CD besteht darin, es Benutzern zu ermöglichen, die CentOS-Funktionen auszuschöpfen, ohne CentOS zu installieren. Die Live-CD wird ohne Auswirkungen auf die Festplatte im Arbeitsspeicher ausgeführt. Änderungen, die Sie in der Laufzeitumgebung der Live-CD vornehmen, gehen nach einem Rechnerneustart verloren.

Diese Live-CD enthält Ihre gesamten Systemeinstellungen und Betriebssystemdateien und kann verwendet werden, um folgende Funktionen auszuführen:

- Sie können Arcserve UDP Agent (Linux) verwenden, ohne das Produkt tatsächlich zu installieren. Dies ermöglicht es Ihnen, das Produkt zu nutzen und auszuwerten, ohne es zu installieren oder Änderungen an der vorhandenen Festplatte Ihres Computers durchzuführen.
- Sie können eine Bare-Metal-Recovery (BMR) ausführen. Sie können diese Live-CD verwenden, um die IP-Adresse des Zielcomputers (der während der BMR erforderlich ist) abzurufen.

Situationen für die Verwendung der CentOS-basierten Live-CD:

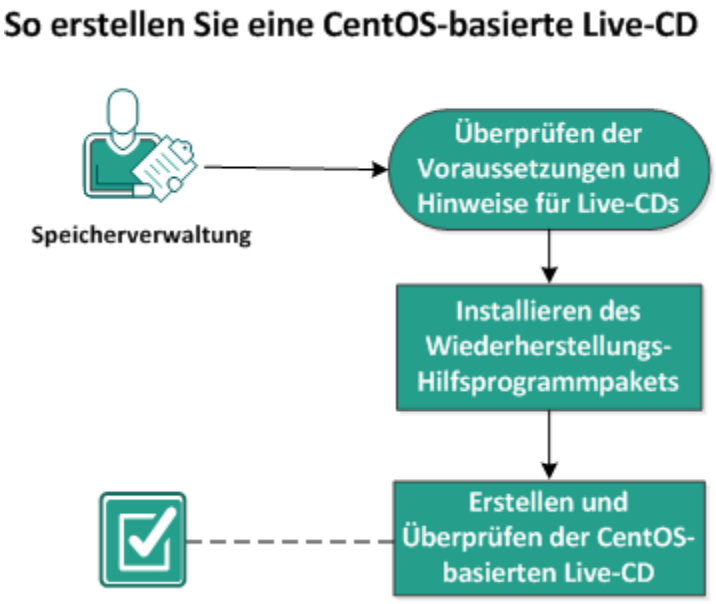
Wenn die standardmäßige Live-CD Speichergerät und Netzwerkgerät aufgrund von fehlenden Gerätetreibern nicht identifizieren kann.

Hinweis: In den Wiederherstellungspunkten, die Sie wiederherstellen möchten, sind die Gerätetreiber für das Speichersystem des Ziel-BMR-Rechners nicht enthalten. Arcserve UDP Agent (Linux) blockiert deswegen alle versuchten BMR-Jobs im Anfangsstadium.

Der Ordner "bin" enthält die Skripte, die Sie von der Befehlszeile ausführen können, um eine startfähige Live-CD zu erstellen. Der Ordner "bin" befindet sich im folgenden Pfad:

```
# /opt/CA/d2dserver/bin
```

Die folgende Abbildung veranschaulicht den Vorgang zur Erstellung einer CentOS-basierten Live-CD:


So erstellen Sie eine CentOS-basierte Live-CD
Speicherverwaltung
Überprüfen der Voraussetzungen und Hinweise für Live-CDs
Installieren des Wiederherstellungs-Hilfsprogrammpakets
Erstellen und Überprüfen der CentOS-basierten Live-CD

Führen Sie die folgenden Aufgaben aus, um eine CentOS-basierte Live-CD zu erstellen:

- Überprüfen der Voraussetzungen und Hinweise für Live-CDs (siehe Seite 103)
- Installieren des Wiederherstellungs-Hilfsprogrammpakets (siehe Seite 105)
- Erstellen und Überprüfen der CentOS-basierten Live-CD (siehe Seite 105)

Überprüfen der Voraussetzungen und Hinweise für Live-CDs

Bevor Sie eine CentOS-basierte Live-CD erstellen, überprüfen Sie die folgende Tabelle, in der die standardmäßige Live-CD mit der CentOS-basierten Live-CD verglichen wird:

Parameter	Standardmäßige Live-CD	CentOS-basierte Live-CD
Installationsdatenträger des Sicherungsservers	Unterstützt	Nicht unterstützt
Desktop-Benutzeroberfläche	Nicht unterstützt. Benutzer müssen einen Browser auf einem Windows-Rechner verwenden, um durch die Webbenutzeroberfläche des Sicherungsservers zu navigieren.	Unterstützt. In der CentOS-basierten Live-CD ist ein Browser enthalten. Benutzer benötigen keinen zusätzlichen Browser, um durch die Webbenutzeroberfläche des Sicherungsservers zu navigieren.

Parameter	Standardmäßige Live-CD	CentOS-basierte Live-CD
Image-Größe	Ca. 400 MB. Das Image kann auf eine CD gebrannt werden.	Über 800 MB. Das Image muss auf eine DVD gebrannt werden.
Zusätzlicher Gerätetreiber für die Live-CD	Nicht unterstützt	Unterstützt
Lokale BMR **(Rechnerwiederherstellung ohne Installation eines weiteren Sicherungsservers)**	Unterstützt	Unterstützt
PXE-Boot-Image	Unterstützt	Nicht unterstützt
Entfernen der CD bzw. das ISO-Image nach Rechnerstart vom BMR-Zielcomputer	Unterstützt	Nicht unterstützt. Die DVD bzw. das ISO-Image muss während der gesamten Wiederherstellung auf dem BMR-Zielcomputer geladen sein, bis der BMR-Job abgeschlossen ist und der Rechner neu gestartet wird.
Betriebssystemumgebung der Live-CD auf Englisch	Ja	Ja. Die Desktop-Benutzeroberfläche verwendet ebenfalls Englisch
Lokalisierte Sprache für die Webbenutzeroberfläche des Sicherungsservers	Ja	Ja
Unterstützte Knotentypen	Physische Rechner, ESX-Server VMware-, RHEV-, OVM- und Citrix Xen-VMs werden unterstützt	Nur physische Rechner und VMware ESX server-VMs werden unterstützt

Beachten Sie die folgenden Voraussetzungen, bevor Sie eine CentOS-basierte Live-CD erstellen:

- Sie haben die folgenden Softwarepakete auf dem Sicherungsserver installiert:
  - genisoimage
  - squashfs-tools
- Die CentOS-basierte Live-CD kann nur von einem physischen Rechner oder einer ESX-Server-VM gestartet werden. Andere Virtualisierungslösungen werden nicht unterstützt.
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Installieren des Wiederherstellungs-Hilfsprogrammpakets

Sie müssen das Wiederherstellungs-Hilfsprogrammpaket installieren, um Wiederherstellungsvorgänge ausführen zu können. Wenn Sie das Wiederherstellungs-Hilfsprogrammpaket nicht installieren, können Sie keine Wiederherstellung auf Dateiebene oder BMR ausführen. Sie können das Wiederherstellungs-Hilfsprogrammpaket während der Installation von Arcserve UDP Agent (Linux) installieren. Sie können das Wiederherstellungs-Hilfsprogrammpaket auch herunterladen und jederzeit nach der Installation von Arcserve UDP Agent (Linux) installieren.

Nachdem Sie das Wiederherstellungs-Hilfsprogrammpaket installiert haben, können Sie eine Live-CD erstellen.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Navigieren Sie mit dem folgenden Befehl zum Ordner "bin":

   ```
   # cd /opt/CA/d2dserver/bin
   ```

3. Führen Sie den folgenden Befehl aus, um das Wiederherstellungs-Hilfsprogrammpaket zu installieren:

   ```
   # ./configutility
   ```

   Eine Meldung wird angezeigt, die Sie dazu auffordert, den Pfad des Wiederherstellungs-Hilfsprogrammpakets anzugeben.

4. Geben Sie den vollständigen Pfad an, wo Sie das Wiederherstellungs-Hilfsprogrammpaket heruntergeladen haben.

   Die Installation wird gestartet.

Das Wiederherstellungs-Hilfsprogrammpaket wird installiert.

Erstellen und Überprüfen der CentOS-basierten Live-CD

Sie können diese Live-CD verwenden, um einen BMR-Zielcomputer zu starten und anschließende den BMR-Job auszuführen. Die folgenden Dateien werden verwendet, um die CentOS-basierte Live-CD zu erstellen:

makelivecd.centos

Ein Skript, das für Remastering der CentOS-Live-CD verwendet wird.

CentOS-6.X-i386-LiveCD.iso

Ein ISO-Image der CentOS-Live-CD. Das Image kann von der CentOS-Website heruntergeladen werden.

Der wiederhergestellte Wiederherstellungspunkt enthält die Gerätetreiber für das Speichersystem des Ziel-BMR-Rechners nicht. Arcserve UDP Agent (Linux) blockiert solche BMR-Jobs in einem frühen Stadium.

Gehen Sie wie folgt vor:

1. Bereiten Sie die Gerätetreiber (*.ko- und *.rpm-Dateien) für CentOS vor, und speichern Sie sie in einem Ordner.

   Beispiel: Speichern Sie die Gerätetreiber im Ordner /tmp/drivers.

   Hinweis: Sie müssen den Gerätetreiber angeben, der mit der Kernel-Version der CentOS-Live-CD übereinstimmt.

2. Gehen Sie zur CentOS-Website, und laden Sie die Live-CD der 32-Bit-Version von CentOS 6.0 oder höher in den Ordner "/tmp" auf dem Sicherungsserver herunter.

   Die Datei "CentOS-6.X-i386-LiveCD.iso" wird heruntergeladen.

3. Navigieren Sie zum Ordner "bin" (/opt/CA/d2dserver/bin), und führen Sie den folgenden Befehl aus:

   ```
   makelivecd.centos <vollständiger_Pfad_zur_CentOS_Live_CD>
   <Pfad_zum_Speicherort_der_Gerätetreiber>
   ```

   Beispiel: makelivecd.centos <vollständiger_Pfad_zur_CentOS_Live_CD> /tmp/drivers

   Das Skript erstellt die auf CentOS basierte Arcserve Unified Data Protection Agent for Linux-Live-CD und speichert die ISO-Image-Datei am folgenden Speicherort:

   ```
   /opt/CA/d2dserver/packages/CentOS-LiveCD-for-D2D.iso
   ```

4. Navigieren Sie zum Paketordner, und stellen Sie sicher, dass die Datei "CentOS-LiveCD-for-D2D.iso" im Ordner enthalten ist.

   Die CentOS-basierte Live-CD wird erstellt und überprüft.

Sie haben erfolgreich eine CentOS-basierte Live-CD erstellt.

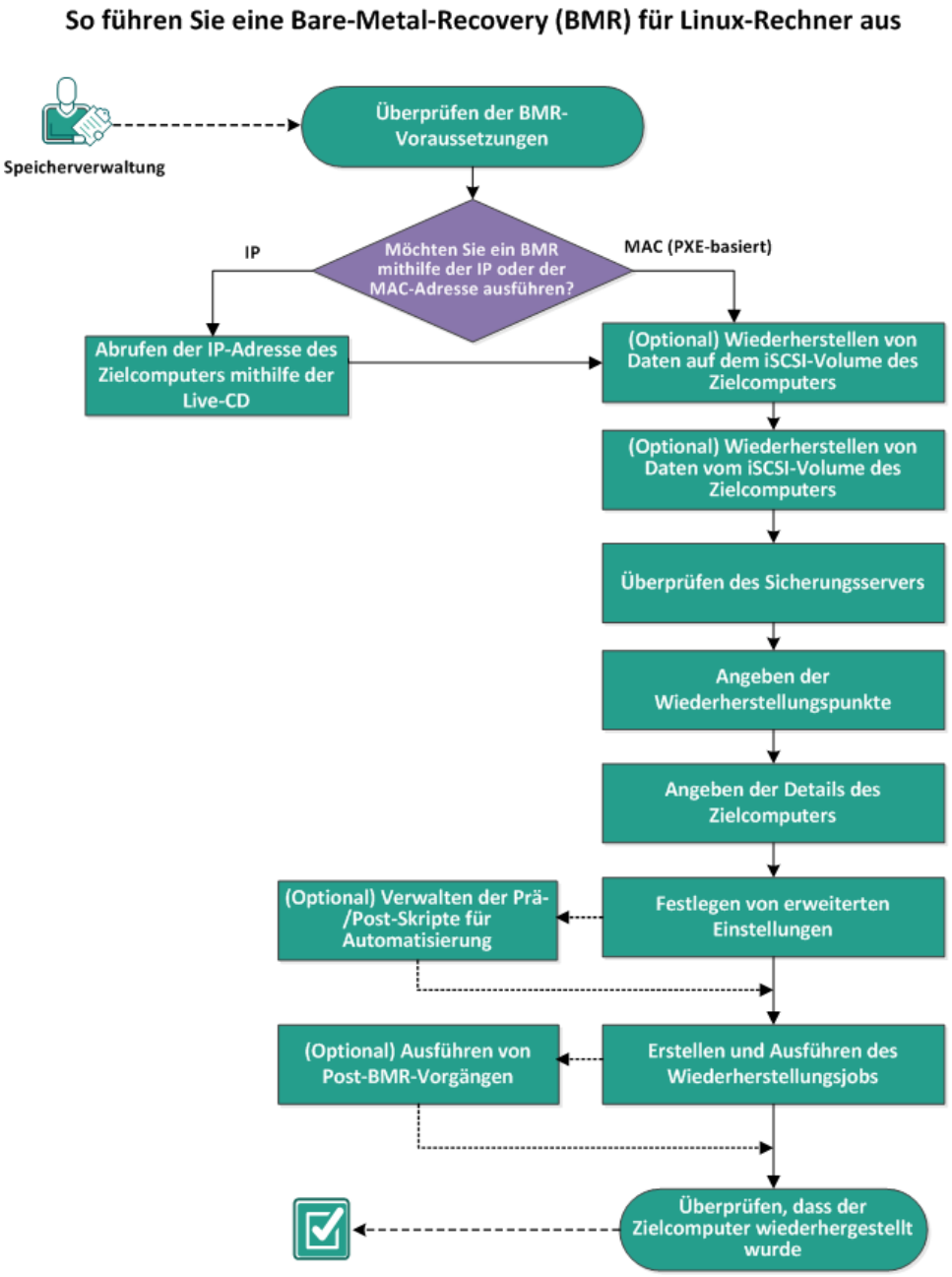
So führen Sie eine Bare-Metal-Recovery (BMR) für Linux-Rechner aus

Eine BMR stellt das Betriebssystem und die Software-Anwendungen sowie alle gesicherten Daten wieder her. Eine BMR ist der Prozess, bei dem ein *Bare-Metal*-Computersystem wiederhergestellt wird. "Bare Metal" bezeichnet einen Computer ohne Betriebssystem, Treiber und Software-Anwendungen. Nachdem die Wiederherstellung abgeschlossen wurde, startet der Zielcomputer automatisch in der gleichen Betriebsumgebung wie der Sicherungsquellknoten neu, und alle Daten werden wiederhergestellt.

Eine vollständige BMR ist möglich, da beim Ausführen einer Sicherung der Daten auch Informationen aufzeichnet werden, die sich auf das Betriebssystem, die installierten Anwendungen, Treiber usw. beziehen.

Sie können eine BMR unter Verwendung der IP-Adresse oder der MAC-Adresse (Media Access Control) des Zielcomputers ausführen. Wenn Sie den Zielcomputer mithilfe der Arcserve UDP Agent (Linux)-Live-CD booten, können Sie die IP-Adresse des Zielcomputers abrufen.

Folgendes Diagramm zeigt den Prozess an, um eine BMR auszuführen:


So führen Sie eine Bare-Metal-Recovery (BMR) für Linux-Rechner aus
Speicherverwaltung
Überprüfen der BMR-Voraussetzungen
Möchten Sie ein BMR mithilfe der IP oder der MAC-Adresse ausführen?
IP
MAC (PXE-basiert)
Abrufen der IP-Adresse des Zielcomputers mithilfe der Live-CD
(Optional) Wiederherstellen von Daten auf dem iSCSI-Volume des Zielcomputers
(Optional) Wiederherstellen von Daten vom iSCSI-Volume des Zielcomputers
Überprüfen des Sicherungsservers
Angeben der Wiederherstellungspunkte
Angeben der Details des Zielcomputers
Festlegen von erweiterten Einstellungen
(Optional) Verwalten der Prä-/Post-Skripte für Automatisierung
Erstellen und Ausführen des Wiederherstellungsjobs
(Optional) Ausführen von Post-BMR-Vorgängen
Überprüfen, dass der Zielcomputer wiederhergestellt wurde

Gehen Sie folgt vor, um eine BMR auszuführen:

- Überprüfen der Voraussetzungen für BMR (siehe Seite 109)
- Abrufen der IP-Adresse des Zielcomputers mithilfe der Live-CD (siehe Seite 110)
- (Optional) Wiederherstellen von Daten auf dem iSCSI-Volume des Zielcomputers (siehe Seite 111)
- (Optional) Wiederherstellen von Daten des iSCSI-Volume des Zielcomputers (siehe Seite 112)
- Überprüfen des Sicherungsservers (siehe Seite 113)
- Angeben der Wiederherstellungspunkte (siehe Seite 114)
- Angeben der Details des Zielcomputers (siehe Seite 117)
- Festlegen von erweiterten Einstellungen (siehe Seite 117)
- (Optional) Verwalten der Prä-/Post-Skripte für Automatisierung (siehe Seite 119)
- Erstellen und Ausführen des Wiederherstellungsjobs (siehe Seite 122)
- (Optional) Ausführen von Post-BMR-Vorgängen (siehe Seite 123)
- Überprüfen, dass der Zielcomputer wiederhergestellt wurde (siehe Seite 129)

Überprüfen der Voraussetzungen

Beachten Sie Folgendes, bevor Sie eine BMR durchführen:

- Sie verfügen über einen gültigen Wiederherstellungspunkt und, falls erforderlich, über das Verschlüsselungskennwort für die Wiederherstellung.
- Sie verfügen über einen gültigen Zielcomputer für die BMR.
- Sie haben die Arcserve UDP Agent (Linux)-Live-CD erstellt.
- Wenn Sie eine BMR mithilfe der IP-Adresse ausführen möchten, müssen Sie die IP-Adresse des Zielcomputers mithilfe der Live-CD abrufen.
- Wenn Sie eine PXE-basierte BMR mithilfe der MAC-Adresse ausführen möchten, müssen Sie die MAC-Adresse des Zielcomputers haben.
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Abrufen der IP-Adresse des Zielcomputers mithilfe der Live-CD

Bevor Sie eine BMR mithilfe der IP-Adresse ausführen können, müssen Sie die IP-Adresse des Zielcomputers ermitteln. Ein Bare-Metal-Computer verfügt anfänglich nicht über eine IP-Adresse. Sie müssen den Bare-Metal-Computer daher mit der Standard-Live-CD (Arcserve UDP Agent (Linux)-Live-CD) oder der CentOS-basierten Live-CD booten, um die IP-Adresse abzurufen. Nachdem Sie die IP-Adresse des Zielcomputers abgerufen haben, können Sie die statische IP des Zielcomputers konfigurieren.

Gehen Sie wie folgt vor:

1. Legen Sie die Live-CD ein oder laden Sie die ISO-Datei der Live-CD im CD-ROM-Laufwerk des Zielknotens.
2. Starten Sie den Zielcomputer von CD-ROM.

   Der Zielcomputer startet in der Umgebung der Arcserve UDP Agent (Linux)-Live-CD. Auf dem Bildschirm wird die IP-Adresse des Zielcomputers angezeigt.
3. Um die statische IP des Zielcomputers mithilfe der Live-CD zu konfigurieren, führen Sie die folgenden Schritte aus:

   a. Drücken Sie im Fenster des Zielcomputers auf die Eingabetaste, um in die Shell-Umgebung zu gelangen.

   b. Führen Sie folgenden Befehl aus, um die statische IP zu konfigurieren:

   ```
   ifconfig <NIC-Name>  <statische IP-Adresse> netmask <Netzmaske>

   route add default  gw  <Gateway-IP-Adresse> <NIC-Name>
   ```

   Hinweis: Der Name Ihrer Netzwerkkarte (NIC) hängt von Ihrer Hardware ab. Typische NIC-Namen sind z. B. "eth0" oder "em0".
4. Um die statische IP des Zielcomputers mithilfe der CentOS-basierten Live-CD zu konfigurieren, führen Sie die folgenden Schritte aus:

   a. Öffnen Sie ein Terminal-Fenster auf dem Zielrechner, indem Sie auf "Anwendungen", "System-Tools", "Terminal" klicken.

   b. Führen Sie die folgenden Befehle aus:

   ```
   sudo ifconfig <NIC-Name>  <statische IP-Adresse> netmask <Netzmaske>

   sudo route add default  gw  <Gateway-IP-Adresse> <NIC-Name>
   ```

   Die statische IP ist konfiguriert.

Die IP-Adresse des Zielcomputers wird erfasst.

Wichtig! Notieren Sie diese IP-Adresse. Sie wird benötigt, wenn Sie die Details des Zielcomputers im **Wiederherstellungsassistenten** angeben müssen.

(Optional) Wiederherstellen von Daten auf dem iSCSI-Volume des Zielcomputers

Sie können das iSCSI-Volume mit dem Zielcomputer integrieren und es zu einem Teil des Zielcomputers machen. Danach können Sie Daten auf dem iSCSI-Volume des Zielcomputers wiederherstellen. Auf diese Weise können Sie Daten über ein Netzwerk verwalten und übertragen.

Wichtig! Wenn Sie das iSCSI-Volume mit dem Zielcomputer integrieren, verlieren Sie sämtliche vorhandenen Daten auf dem iSCSI-Volume.

Gehen Sie wie folgt vor:

1. Legen Sie die Arcserve UDP Agent (Linux)-Live-CD ein bzw. laden Sie die ISO-Datei der Arcserve UDP Agent (Linux)-Live-CD im CD-ROM-Laufwerk des Zielcomputers.
2. Starten Sie den Zielcomputer über die CD-ROM.

   Der Zielcomputer startet in der Umgebung der Arcserve UDP Agent (Linux)-Live-CD. Auf dem Bildschirm wird die IP-Adresse des Zielcomputers angezeigt.
3. Geben Sie die Shell-Umgebung des Zielcomputers ein.
4. Führen Sie den folgenden Befehl aus, den iSCSI-Initiator-Daemon zu starten:

   ```
   /etc/init.d/iscsid start
   ```
5. Führen Sie ein Discovery-Skript aus, um den iSCSI-Zielhost zu erkennen.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADRESSE>:<Portnummer>
   ```

   Der Standardportwert des iSCSI-Zielhost ist 3260.
6. Notieren Sie den iSCSI Qualified Name (IQN) des iSCSI-Zielhost, der durch das Discovery-Skript gefunden wird, bevor Sie sich manuell beim erkannten Zielcomputer anmelden.
7. Listen Sie das verfügbare Blockgerät des Zielknotens auf.

   ```
   #fdisk -l
   ```
8. Melden Sie sich beim erkannten Ziel an.

   ```
   iscsiadm -m node -T <iSCSI Target IQN name> -p
   <ISCSI-SERVER-IP-ADRESSE>:<Portnummer> -l
   ```

   Im Verzeichnis /dev des Zielknotens wird ein Blockgerät angezeigt.
9. Führen Sie den folgenden Befehl aus, um den Namen des neuen Geräts abzurufen:

   ```
   #fdisk –l
   ```

   Im Zielknoten können Sie ein zusätzliches Gerät, /dev/sd<x>, sehen.

Das iSCSI-Volume wurde mit dem Ziel-Volume integriert.

(Optional) Wiederherstellen von Daten des iSCSI-Volume des Zielcomputers

Wenn Sie Ihre Daten auf einem iSCSI-Zieldatenträger gespeichert haben, können Sie eine Verbindung mit dem iSCSI-Volume herstellen und Daten wiederherstellen. Das iSCSI-Volume ermöglicht das Verwalten und Übertragen von Daten über ein Netzwerk.

Gehen Sie wie folgt vor:

1. Legen Sie die Arcserve UDP Agent (Linux)-Live-CD ein bzw. laden Sie die ISO-Datei der Arcserve UDP Agent (Linux)-Live-CD im CD-ROM-Laufwerk des Zielcomputers.
2. Starten Sie den Zielcomputer über die CD-ROM.

   Der Zielcomputer startet in der Umgebung der Arcserve UDP Agent (Linux)-Live-CD. Auf dem Bildschirm wird die IP-Adresse des Zielcomputers angezeigt.
3. Geben Sie die Shell-Umgebung des Zielcomputers ein.
4. Führen Sie den folgenden Befehl aus, den iSCSI-Initiator-Daemon zu starten:

   ```
   /etc/init.d/iscsid start
   ```
5. Führen Sie ein Discovery-Skript aus, um den iSCSI-Zielhost zu erkennen.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADRESSE>:<Portnummer>
   ```

   Der Standardportwert des iSCSI-Zielhost ist 3260.
6. Notieren Sie den iSCSI Qualified Name (IQN) des iSCSI-Zielhost, der durch das Discovery-Skript gefunden wird, bevor Sie sich manuell beim erkannten Zielcomputer anmelden.
7. Listen Sie das verfügbare Blockgerät des Zielknotens auf.

   ```
   #fdisk -l
   ```
8. Melden Sie sich beim erkannten Ziel an.

   ```
   iscsiadm -m node -T <iSCSI Target IQN name> -p
   <ISCSI-SERVER-IP-ADRESSE>:<Portnummer> -l
   ```

   Im Verzeichnis /dev des Zielknotens wird ein Blockgerät angezeigt.
9. Führen Sie den folgenden Befehl aus, um den Namen des neuen Geräts abzurufen:

   ```
   #fdisk –l
   ```

   Im Zielknoten können Sie ein zusätzliches Gerät, /dev/sd<x>, sehen.

   In diesem Beispiel ist der Name des Geräts "/dev/sdc". In den folgenden Schritten wird dieser Gerätename verwendet, um eine Partition und ein Dateisystem zu erstellen.

10. Laden Sie das iSCSI-Volume mithilfe der folgenden Befehle:

    ```
    # mkdir /iscsi

    # mount /dev/sdc1 /iscsi
    ```

    Hinweis: Wenn Sie den Sitzungsspeicherort im Wiederherstellungsassistenten angeben, müssen Sie "Lokal" auswählen und den Pfad /iscsi eingeben.

    Beispiel: <Pfad>/iscsi

Der Zielcomputer kann jetzt eine Verbindung mit dem iSCSI-Volume herstellen und Daten vom iSCSI-Volume wiederherstellen.

Überprüfen des Sicherungsservers

Wenn Sie den **Wiederherstellungsassistenten** öffnen, überprüfen Sie den Sicherungsserver, auf dem die Wiederherstellung ausgeführt werden soll.

Gehen Sie wie folgt vor:

1. Führen Sie einen der folgenden Vorgänge durch, um auf den Wiederherstellungs-Assistenten zuzugreifen:
   - In Arcserve UDP:
     a. Melden Sie sich bei Arcserve UDP an.
     b. Klicken Sie auf die Registerkarte **Ressourcen**.
     c. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

        Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.
     d. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Aktionen**.
     e. Klicken Sie im Drop-down-Menü **Aktionen** auf **Wiederherstellen**.

        Die Arcserve UDP Agent (Linux)-Webbenutzeroberfläche wird geöffnet. Das Auswahldialogfeld für den Wiederherstellungstyp wird in der Benutzeroberfläche des Agenten angezeigt.
     f. Wählen Sie den Wiederherstellungstyp aus, und klicken Sie auf **OK**.

        Hinweis: Sie werden automatisch beim Agentenknoten angemeldet, und der **Wiederherstellungsassistent** wird im Agentenknoten geöffnet.
   - In Arcserve UDP Agent (Linux):
     a. Öffnen Sie die Arcserve UDP Agent (Linux)-Webbenutzeroberfläche.

        Hinweis: Während der Installation von Arcserve UDP Agent (Linux) haben Sie die URL erhalten, um auf den Server zugreifen und ihn verwalten zu können. Melden Sie sich bei Arcserve UDP Agent (Linux) an.

b. Klicken Sie auf "**Wiederherstellen**" im Menü "**Assistent**", und wählen Sie "**Bare-Metal-Recovery (BMR)**" aus.

Die Seite **Sicherungsserver** in **Wiederherstellungsassistent - BMR** wird geöffnet.

2. Überprüfen Sie den Server in der Drop-down-Liste **Sicherungsserver** auf der Seite **Sicherungsserver**.

   Sie können in der Drop-down-Liste **Sicherungsserver** keine Optionen auswählen.

3. Klicken Sie auf "**Weiter**".

   Die Seite "**Wiederherstellungspunkte**" des **Wiederherstellungs-Assistenten - BMR** wird geöffnet.

Der Sicherungsserver wird angegeben.

Angeben der Wiederherstellungspunkte

Bei jedem Ausführen einer Sicherung wird ein Wiederherstellungspunkt erstellt. Geben Sie die Informationen zu den Wiederherstellungspunkten im **Wiederherstellungsassistenten** an, damit genau die gewünschten Daten wiederhergestellt werden. Sie können je nach Bedarf bestimmte Dateien oder alle Dateien wiederherstellen.

Wichtig! Um eine BMR von einem Wiederherstellungspunkt ausführen zu können, müssen das root-Volume und das Startvolume im Wiederherstellungspunkt vorhanden sein.

Gehen Sie wie folgt vor:

1. Führen Sie je nach Sicherungsspeicher einen der folgenden Schritte aus.

   - Führen Sie folgende Schritte aus, um auf Wiederherstellungspunkte zuzugreifen, wenn die Wiederherstellungspunkte auf einem mobilen Gerät gespeichert sind:

     a. Starten Sie den Zielcomputer mithilfe der Live-CD.

     b. Melden Sie sich über die Live-CD bei der Arcserve UDP Agent (Linux)-Webschnittstelle an.

     c. Öffnen Sie den **BMR-Assistenten**.

     d. Navigieren Sie zur Seite **Wiederherstellungspunkte**.

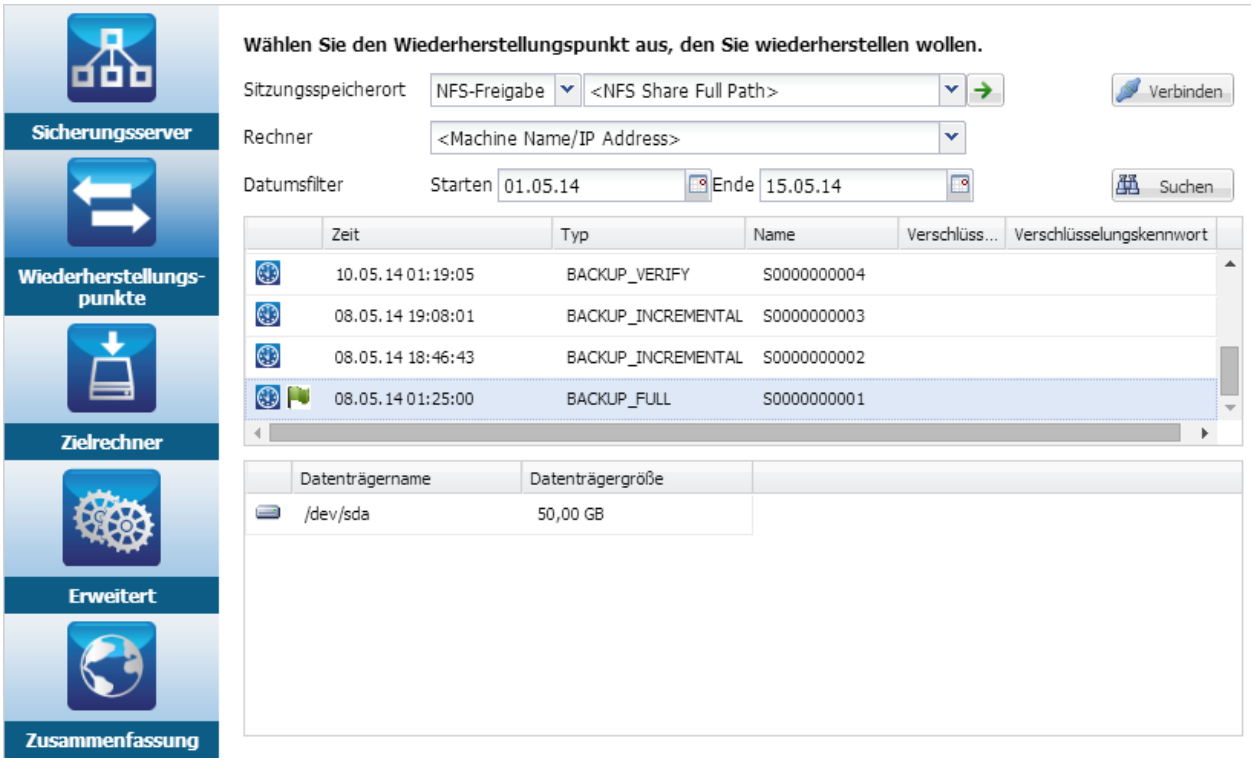
     e. Wählen Sie auf der Seite **Wiederherstellungspunkte** des **BMR-Assistenten** als **Sitzungsspeicherort Lokal** aus.

   - Führen Sie folgende Schritte aus, wenn der Sitzungsspeicherort "NFS-Freigabe" oder "CIFS-Freigabe" ist:

     a. Wählen Sie in der Drop-down-Liste "**Sitzungsspeicherort**" eine Sitzung aus, und geben Sie den vollständigen Pfad der Freigabe ein.

        Nehmen Sie zum Beispiel an, dass der Sitzungsspeicherort eine NFS-Freigabe, xxx.xxx.xxx.xxx die IP-Adresse der NFS-Freigabe und der Ordnernamen "*Daten*" ist. Sie geben dann "xxx.xxx.xxx.xxx:/Data" als Speicherort der NFS-Freigabe an.

     Hinweis: Wenn die gesicherten Daten unter "Quelle - lokal" gespeichert werden, müssen Sie den Quellknoten zuerst in einen NFS-Server konvertieren und dann den Sitzungsspeicherort freigeben.



2. Klicken Sie auf "**Verbinden**".

   Alle Knoten, die an diesem Speicherort gesichert wurden, werden in der Drop-down-Liste "**Rechner**" aufgelistet.

3. Wählen Sie den Knoten, von dem Sie eine Wiederherstellung vornehmen möchten, in der Drop-down-Liste "**Rechner**" aus.

   Es werden alle Wiederherstellungspunkte des ausgewählten Knotens aufgelistet.

4. Wenden Sie den Datumsfilter an, um die Wiederherstellungspunkte anzuzeigen, die zwischen dem angegebenen Datum generiert werden, und klicken Sie auf **Suchen**.

   Standard: Die letzten zwei Wochen.

   Alle verfügbaren Wiederherstellungspunkte zwischen den angegebenen Datumswerten werden angezeigt.

5. Wählen Sie den gewünschten Wiederherstellungspunkt aus, und klicken Sie auf "**Weiter**".

   Die Seite "**Zielcomputer**" wird geöffnet.

Der Wiederherstellungspunkt wird angegeben.

Angeben der Details des Zielcomputers

Geben Sie die Details des Zielcomputers an, damit Daten auf diesem Rechner wiederhergestellt werden. Ein Zielcomputer ist ein Bare-Metal-Rechner, auf dem Sie eine BMR ausführen. Wenn Sie mithilfe der IP-Adresse wiederherstellen, benötigen Sie die IP-Adresse des Zielcomputers, die Sie zu Beginn dieses Prozesses notiert haben. Wenn Sie mithilfe der MAC-Adresse (Media Access Control) wiederherstellen, benötigen Sie die MAC-Adresse des Zielcomputers.

Gehen Sie wie folgt vor:

1. Geben Sie die MAC-Adresse oder die IP-Adresse des Zielcomputers im Feld **MAC-/IP-Adresse** ein.
2. Geben Sie einen Namen in das Feld **Hostname** ein.

   Der Zielcomputer verwendet diesen Namen als Hostnamen, wenn die Wiederherstellung abgeschlossen ist.
3. Wählen Sie eine der folgenden Optionen als Netzwerk aus:

   DHCP

   Konfiguriert die IP-Adresse automatisch. Dies ist die Standardoption. Verwenden Sie diese Option, wenn Sie über einen DHCP-Server (Dynamic Host Configuration Protocol) verfügen, um über die Wiederherstellung über das DHCP-Netzwerk auszuführen.

   Statische IP

   Konfiguriert die IP-Adresse manuell. Wenn Sie diese Option auswählen, geben Sie **IP-Adresse**, **Subnetzmaske** und **Standard-Gateway** des Zielcomputers ein.

   Wichtig! Stellen Sie sicher, dass die statische IP von keinen anderen Rechnern im Netzwerk verwendet wird, während die Wiederherstellung durchgeführt wird.
4. (Optional) Wählen Sie die Option **Neu starten** aus, um den Zielknoten nach Abschluss der BMR neu zu starten.
5. Klicken Sie auf "**Weiter**".

   Das Dialogfeld **"Erweitert"** wird geöffnet.

Die Details des Zielcomputers sind angegeben.

Festlegen von erweiterten Einstellungen

Geben Sie die erweiterten Einstellungen an, um eine geplante BMR der Daten auszuführen. Mit einer geplanten BMR wird sichergestellt, dass die Daten auch bei Ihrer Abwesenheit zur angegebenen Zeit wiederhergestellt werden.

Gehen Sie wie folgt vor:

1. Legen Sie Datum und Uhrzeit für den Beginn fest, indem Sie eine der folgenden Optionen auswählen:

   Jetzt ausführen

   Startet den Wiederherstellungsjob sofort, nachdem Sie den Job übergeben haben.

   Spezielle Zeit festlegen

   Startet den Wiederherstellungsjob zur angegebenen Zeit, nachdem Sie den Job übergeben haben.

2. (Optional) Wählen Sie ein Skript aus der Option "**Einstellungen für Prä-/Post-Skripts**" für den Sicherungsserver und den Zielcomputer aus.

   Diese Skripte führen Skriptbefehle für Aktionen aus, die vor dem Start des Jobs und/oder nach Abschluss des Jobs durchgeführt werden sollen.

   Hinweis: Die Felder für **Einstellungen vor/nach dem Skript** werden nur aufgefüllt, wenn Sie bereits eine Skriptdatei erstellt und an folgendem Speicherort platziert haben:

   ```
   /opt/CA/d2dserver/usr/prepost
   ```

   Hinweis: Weitere Informationen zur Erstellung der Prä-/Post-Skripte finden Sie unter *Verwalten der Prä-/Post-Skripte für Automatisierung* (siehe Seite 156).

3. (Optional) Klicken Sie auf "**Weitere Einstellungen anzeigen**", um weitere Einstellungen für die BMR anzuzeigen.

4. (Optional) Setzen Sie das Kennwort für den angegebenen Benutzernamen des wiederhergestellten Zielcomputers zurück.

5. (Optional) Geben Sie den vollständigen Pfad des Sicherungsspeicherorts der Wiederherstellungspunkte unter "**Wiederherstellungspunkt - Lokaler Zugriff**" an.

6. (Optional) Geben Sie den vollständigen Namen des Datenträgers im Feld "**Datenträger**" ein, um diese Datenträger auf dem Zielcomputer von der Wiederherstellung auszuschließen.

7. (Optional) Wählen Sie "**Wake-on-LAN aktivieren**", wenn Sie eine PXE-BMR (Preboot Execution Environment) ausführen.

   Hinweis: Die Option **Wake-on-LAN aktivieren** kann nur auf physische Rechner angewendet werden. Stellen Sie sicher, ob Sie die Wake-on-LAN-Einstellungen in den BIOS-Einstellungen Ihres physischen Rechners aktiviert haben.

8. Klicken Sie auf "**Weiter**".

   Die Seite **"Zusammenfassung"** wird geöffnet.

Die erweiterten Einstellungen sind angegeben.

(Optional) Verwalten der Prä-/Post-Skripte für Automatisierung

Mit Prä-/Post-Skripts können Sie Ihre eigene Geschäftslogik in bestimmten Phasen eines in Bearbeitung befindlichen Jobs ausführen. Sie können in **Einstellungen vor/nach dem Skript** des **Sicherungsassistenten** und des **Wiederherstellungsassistenten** auf der Benutzeroberfläche angeben, wann Ihre Skripte ausgeführt werden sollen. Die Skripts können je nach Einstellung auf dem Sicherungsserver ausgeführt werden.

Das Verwalten von Prä-/Post-Skripts ist ein zweiteiliger Vorgang, der das Erstellen des Prä-/Post-Skripts und das Einfügen des Skripts in den "prepost"-Ordners umfasst.

Erstellen von Prä-/Post-Skripts

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Erstellen Sie eine Skriptdatei, indem Sie die Umgebungsvariablen in Ihrer bevorzugten Skripterstellungssprache verwenden.

   Umgebungsvariablen des Prä-/Post-Skripts

   Verwenden Sie die folgenden Umgebungsvariablen, um Ihr Skript zu erstellen:

   D2D_JOBNAME

   Gibt den Namen des Jobs an.

   D2D_JOBID

   Gibt die Job-ID an. Die Job-ID ist eine Nummer, die für den Job vergeben wird, wenn Sie den Job ausführen. Wenn Sie den gleichen Job erneut ausführen, erhalten Sie eine neue Jobnummer.

   D2D_TARGETNODE

   Identifiziert den Knoten, der gesichert oder wiederhergestellt wird.

   D2D_JOBTYPE

   Identifiziert den Typ des ausgeführten Jobs. Die folgenden Werte identifizieren die D2D_JOBTYPE-Variable:

   backup.full

   Identifiziert den Job als eine vollständige Sicherung.

   backup.incremental

   Identifiziert den Job als eine Zuwachssicherung.

   backup.verify

   Identifiziert den Job als eine Überprüfungssicherung.

restore.bmr

Identifiziert den Job als eine Bare-Metal-Recovery (BMR). Dies ist ein Wiederherstellungsjob.

restore.file

Identifiziert den Job als eine Wiederherstellung auf Dateiebene. Dies ist ein Wiederherstellungsjob.

D2D_SESSIONLOCATION

Identifiziert den Speicherort, an dem die Wiederherstellungspunkte gespeichert sind.

D2D_PREPOST_OUTPUT

Identifiziert eine Temp-Datei. Der Inhalt der Anfangszeile der Temp-Datei wird im Aktivitätsprotokoll angezeigt.

D2D_JOBSTAGE

Gibt die Phase des Jobs an. Die folgenden Werte identifizieren die D2D_JOBSTAGE-Variable:

pre-job-server

Identifiziert das Skript, das auf dem Sicherungsserver ausgeführt wird, bevor der Job startet.

post-job-server

Identifiziert das Skript, das auf dem Sicherungsserver ausgeführt wird, nachdem der Job abgeschlossen ist.

pre-job-target

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, bevor der Job startet.

post-job-target

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, nachdem der Job abgeschlossen ist.

pre-snapshot

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, bevor der Snapshot erfasst wird.

post-snapshot

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, nachdem der Snapshot erfasst wird.

D2D_TARGETVOLUME

Identifiziert das Volume, das während eines Sicherungsjobs gesichert wird. Diese Variable ist anwendbar für Prä-/Post-Snapshot-Skripts für einen Sicherungsjob.

D2D_JOBRESULT

Identifiziert das Ergebnis für ein Post-Job-Skript. Die folgenden Werte identifizieren die D2D_JOBRESULT-Variable:

success

Identifiziert das Ergebnis als erfolgreich.

fail

Identifiziert das Ergebnis als nicht erfolgreich.

D2DSVR_HOME

Identifiziert den Ordner, in dem der Sicherungsserver installiert ist. Diese Variable ist anwendbar für die Skripts, die auf dem Sicherungsserver ausgeführt werden.

Das Skript ist erstellt.

Hinweis: Bei allen Skripten zeigt der Rückgabewert von Null eine erfolgreiche Erstellung an, und ein Rückgabewert, der ungleich Null ist, weist auf einen Fehler hin.

Überprüfung des Skripts in den Ordner "Prepost" und Überprüfung des Skripts

Alle Prä-/Post-Skripts für einen Sicherungsserver werden zentral vom Ordner "prepost" am folgenden Speicherort verwaltet:

```
/opt/CA/d2dserver/usr/prepost
```

Gehen Sie wie folgt vor:

1. Fügen Sie die Datei in folgenden Speicherort des Sicherungsservers ein:

   ```
   /opt/CA/d2dserver/usr/prepost
   ```

2. Geben Sie der Skriptdatei Ausführungsberechtigungen.
3. Melden Sie sich bei der Arcserve UDP Agent (Linux)-Webbenutzeroberfläche an.
4. Öffnen Sie den **Sicherungsassistenten** oder **Wiederherstellungsassistenten**, und navigieren Sie zur Registerkarte **Erweitert**.
5. Wählen Sie die Skriptdatei in der Drop-down-Liste **Einstellungen vor/nach dem Skript** aus, und übergeben Sie den Job.
6. Klicken Sie auf "**Aktivitätsprotokoll**", und stellen Sie sicher, dass das Skript für den angegebenen Sicherungsjob ausgeführt wird.

   Das Skript wird ausgeführt.

Die Prä-/Post-Skripte wurden erfolgreich erstellt und befinden sich im Ordner "prepost".

Erstellen und Ausführen des Wiederherstellungsjobs

Erstellen Sie den Wiederherstellungsjob, und führen Sie ihn aus, sodass Sie den BMR-Prozess initiieren können. Überprüfen Sie die Wiederherstellungspunktinformationen, bevor Sie eine BMR ausführen. Bei Bedarf können Sie zurückgehen und die Wiederherstellungseinstellungen ändern.

Gehen Sie wie folgt vor:

1. Überprüfen Sie die Wiederherstellungsdetails auf der Seite **Zusammenfassung** des **Wiederherstellungsassistenten**.
2. (Optional) Klicken Sie auf **Zurück**, um die Wiederherstellungseinstellungen auf den Seiten des **Wiederherstellungsassistenten** zu ändern.
3. Geben Sie einen Jobnamen ein, und klicken Sie auf "**Übergeben**".

   Im Feld "**Jobname**" ist zunächst ein Standardname angegeben. Sie können einen neuen Jobnamen Ihrer Wahl eingeben, wobei das Feld jedoch nicht leer gelassen werden darf.

   Der **Wiederherstellungsassistent** wird geschlossen. Der Job wird auf der Registerkarte "**Jobstatus**" angezeigt. Wenn Sie die IP-Adresse für die BMR verwenden, startet der Zielcomputer nach dem BMR-Prozess automatisch auf dem gleichen Betriebssystem wie die Sicherungsquelle neu.

   Wenn Sie die MAC-Adresse für die BMR verwenden, ändert sich der Status auf der Registerkarte "**Jobstatus**" in "*Es wird auf das Starten des Zielknotens gewartet*".
4. (Optional) Wenn Sie eine BMR mithilfe der MAC-Adresse ausführen, gehen Sie wie folgt vor: Starten Sie den Zielcomputer, wenn die Meldung "*Es wird auf das Starten des Zielknotens gewartet*" auf der Registerkarte "**Jobstatus**" angezeigt wird.

   Hinweis: Wenn der Zielcomputer bereits gestartet wurde, bevor Sie den Wiederherstellungsjob übergeben, müssen Sie den Zielcomputer neu starten. Stellen Sie sicher, dass BIOS so konfiguriert ist, dass vom Netzwerk gestartet wird.

   Der Status in der Spalte **Jobstatus** wird in **Volume wird wiederhergestellt** umgeändert. Dies gibt an, dass die Wiederherstellung in Bearbeitung ist. Nachdem der Wiederherstellungsjob abgeschlossen wurde, startet der Zielcomputer automatisch mit dem gleichen Betriebssystem wie die Sicherungsquelle neu.

Der Wiederherstellungsjob wurde erfolgreich erstellt und ausgeführt.

(Optional) Ausführen von Post-BMR-Vorgängen

Folgende Themen sind optionale Konfigurationseinstellungen, die Sie möglicherweise nach einer BMR ausführen müssen:

Konfigurieren von X Windows

Wenn Sie eine BMR über verschiedene Hardware ausführen, funktioniert X Windows des wiederhergestellten BS nicht richtig, und der Zielknoten zeigt ein Fehlerdialogfeld an. Das Fehlerdialogfeld wird angezeigt, weil die Anzeigekonfiguration geändert wurde. Um diesen Fehler zu beheben, folgen Sie den Anweisungen im Fehlerdialogfeld, um die Grafikkarte zu konfigurieren. Danach werden X Windows und die Desktop-Benutzeroberfläche angezeigt.

Konfigurieren Sie den FQDN (Fully Qualified Domain Name) des Systems

Wenn Sie einen FQDN benötigen, dann müssen Sie den FQDN konfigurieren. Der BMR-Prozess konfiguriert den FQDN nicht automatisch.

Maximale Zeichenanzahl für FQDN: 63

Führen Sie diese Schritte aus, um den FQDN zu konfigurieren:

1. Bearbeiten Sie die Datei */etc/hosts*, und geben Sie die IP-Adresse, den FQDN-Namen und den Servernamen an.

   ```
   #vi /etc/hosts

   ip_of_system  servername.domainname.com  servername
   ```

2. Starten Sie den Netzwerkdienst neu.

   ```
   #/etc/init.d/network restart
   ```

3. Überprüfen Sie den Hostnamen und den FQDN-Namen.

   ```
   #hostname

   servername

   #hostname -f

   servername.domainname.com
   ```

Der FQDN ist konfiguriert.

Erweitern des Daten-Volume nach einer BMR auf verschiedenen Datenträgern

Wenn Sie eine BMR auf einem Datenträger ausführen, der größer ist als der Datenträger auf dem ursprünglichen Knoten, dann wird etwas Festplattenspeicher frei gelassen. Der BMR-Vorgang verarbeitet den freien Festplattenspeicher nicht automatisch. Sie können den Festplattenspeicher in eine separate Partition formatieren, oder Sie können die Größe der vorhandenen Partition mit dem freien Festplattenspeicher anpassen. Das Volume, dessen Größe Sie anpassen möchten, muss ungenutzt sein, sodass Sie die Größenänderung eines Systemvolumes vermeiden müssen. In diesem Abschnitt wird erläutert, wie ein Datenvolume mit dem freien Festplattenspeicher erweitert wird.

Hinweis: Um Datenverlust zu vermeiden, passen Sie die Größe Ihrer Volumes sofort nach dem BMR-Prozess an. Sie können auch den Knoten sichern, bevor Sie mit der Größenänderung des Volumes starten.

Wenn der Zielcomputer nach der BMR erfolgreich neu startet, dann können Sie das Datenvolume erweitern.

Rohes Partitionsvolume

Zum Beispiel wird ein 2 GB-Datenträger in der Sitzung in einen 16 GB-Datenträger mit dem Namen */dev/sdb* mit nur einer Partition wiederhergestellt. Die rohe Partition */dev/sdb1* wird direkt in das Verzeichnis */data* geladen.

Dieses Beispiel wird verwendet, um den Vorgang zur Erweiterung des rohen Partitionsvolume zu erläutern.

Folgen Sie diesen Schritten:

1. Überprüfen Sie den Status des Volumes "/dev/sdb1".

```
# df –h /dev/sdb1
/dev/sdb1             2.0G   40M  1.9G   3% /data
```

2. Entladen Sie das Volume "dev/sdb1".

```
# umount /data
```

3. Ändern Sie die Größe von "dev/sdb1", um den gesamten Festplattenspeicher mithilfe des Befehls "fdisk" zu belegen.

   Um diesen Vorgang auszuführen, löschen Sie zuerst Ihre vorhandene Partition, und stellen Sie sie anschließend mit der gleichen Startsektorzahl wieder her. Die gleiche Startsektorzahl ist für die Verhinderung des Datenverlustes verantwortlich.

```
# fdisk -u /dev/sdb

Command (m for help): p

Disk /dev/sdb: 17.1 GB, 17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total 33554432 sectors

Units = sectors of 1 * 512 = 512 bytes

Device Boot      Start         End      Blocks   Id  System

/dev/sdb1              63     4192964     2096451   83  Linux

Command (m for help): d

Selected partition 1

Command (m for help): n

Command action

e   extended

p   primary partition (1-4)

p

Partition number (1-4): 1

First sector (63-33554431, default 63):

Using default value 63

Last sector or +size or +sizeM or +sizeK (63-33554431, default 33554431):

Using default value 33554431

Command (m for help): p

Disk /dev/sdb: 17.1 GB, 17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total 33554432 sectors

Units = sectors of 1 * 512 = 512 bytes
```

```
Device Boot      Start         End      Blocks   Id  System
/dev/sdb1              63    33554431    16777184+  83  Linux
Command (m for help): w
```

Die Partition wird in die gleiche Startsektorzahl wie die ursprüngliche Partition geändert, und die Endsektorzahl ist 33554431.

4. Ändern Sie die Größe des Volumes mithilfe des Befehls "resize2fs". Führen Sie im Bedarfsfall zuerst den Befehl "e2fsck" aus.

```
# e2fsck -f /dev/sdb1
# resize2fs /dev/sdb1
```

5. Laden Sie das Volume auf den Bereitstellungspunkt, und überprüfen Sie den Status des Volumes erneut.

```
# mount /dev/sdb1 /data
# df –h /dev/sdb1
/dev/sdb1              16G   43M   16G   1% /data
```

Das Volume wird auf 16 GB erweitert und kann verwendet werden.

LVM-Volume:

Zum Beispiel wird ein 8 GB-Datenträger in der Sitzung in einen 16 GB-Datenträger mit dem Namen */dev/sdc* mit nur einer Partition wiederhergestellt. Die rohe Partition */dev/sdc1* wird als einziges physisches Volume des LVM-logischen Volumes */dev/mapper/VGTest-LVTest* verwendet, dessen Bereitstellungspunkt */lvm* ist.

Dieses Beispiel wird verwendet, um den Vorgang zur Erweiterung des LVM-Volumes zu erläutern.

Folgen Sie diesen Schritten:

1. Überprüfen Sie den Status des Volumes "/dev/mapper/VGTest-LVTest".

```
# lvdisplay –m /dev/mapper/VGTest-LVTest
--- Logical volume ---
LV Name                /dev/VGTest/LVTest
VG Name                VGTest
LV UUID                udoBIx-XKBS-1Wky-3FVQ-mxMf-FayO-tpfPl8
LV Write Access        read/write
```

```
LV Status              available
# open                 1
LV Size                7.88 GB
Current LE             2018
Segments               1
Allocation             inherit
Read ahead sectors     0
Block device           253:2
---Segments---
Logical extent 0 to 2017:
Type                linear
Physical volume     /dev/sdc1
Physical extents    0 to 2017
```

Das physische Volume ist */dev/sdc1*, die Volume-Gruppe ist *VGTest*, und das logische Volume ist */dev/VGTest/LVTest oder /dev/mapper/VGTest-LVTest*.

2. Entladen Sie das Volume "/dev/mapper/VGTest-LVTest".

```
# umount /lvm
```

3. Deaktivieren Sie die Volume-Gruppe, in der sich das physische Volume "/dev/sdc1" befindet.

```
# vgchange -a n VGTest
```

4. Erstellen Sie eine Partition, um den freien Festplattenspeicher mithilfe des Befehls "fdisk" zu belegen.

```
# fdisk -u /dev/sdc
Command (m for help): p
Disk /dev/sdc: 17.1 GB, 17179869184 bytes
255 heads, 63 sectors/track, 2088 cylinders, total 33554432 sectors
Units = sectors of 1 * 512 = 512 bytes
Device Boot      Start         End      Blocks   Id  System
/dev/sdc1              63    16777215     8388576+  83  Linux
Command (m for help): n
Command action
e   extended
p   primary partition (1-4)
p
```

```
Partition number (1-4): 2

First sector (16777216-33554431, default 16777216):

Using default value 16777216

Last sector or +size or +sizeM or +sizeK (16777216-33554431, default
33554431):

Using default value 33554431

Command (m for help): p

Disk /dev/sdc: 17.1 GB, 17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total 33554432 sectors

Units = sectors of 1 * 512 = 512 bytes

Device Boot      Start         End      Blocks   Id  System

/dev/sdc1              63    16777215     8388576+  83  Linux

/dev/sdc2        16777216    33554431     8388608   83  Linux

Command (m for help): w
```

Die Partition "/dev/sdc2" ist erstellt.

5. Erstellen Sie ein neues physisches Volume.

   ```
   # pvcreate /dev/sdc2
   ```

6. Erweitern Sie die Größe der Volumegruppe.

   ```
   # vgextend VGTest /dev/sdc2
   ```

7. Geben Sie die Volumegruppe frei, die Sie bereits deaktiviert haben.

   ```
   # vgchange -a y VGTest
   ```

8. Erweitern Sie die logische Volumengröße mithilfe des Befehls "lvextend".

   ```
   # lvextend -L +8G /dev/VGTest/LVTest
   ```

9. Ändern Sie die Größe des Volumes mithilfe des Befehls "resize2fs". Führen Sie im Bedarfsfall zuerst den Befehl "e2fsck" aus.

   ```
   # e2fsck -f /dev/mapper/VGTest-LVTest

   # resize2fs /dev/mapper/VGTest-LVTest
   ```

10. Laden Sie das Volume auf den Bereitstellungspunkt, und überprüfen Sie den Status des Volumes erneut.

    ```
    # mount /dev/mapper/VGTest-LVTest /lvm

    # lvdisplay -m /dev/mapper/VGTest-LVTest

    ---Logical volume---

    LV Name                /dev/VGTest/LVTest

    VG Name                VGTest
    ```

```
LV UUID                GTP0a1-kUL7-WUL8-bpbM-9eTR-SVzl-WgA11h
LV Write Access        read/write
LV Status              available
# open                 0
LV Size                15.88 GB
Current LE             4066
Segments               2
Allocation             inherit
Read ahead sectors     0
Block device           253:2
--- Segments ---
Logical extent 0 to 2046:
Type                linear
Physical volume     /dev/sdc1
Physical extents    0 to 2046
Logical extent 2047 to 4065:
Type                linear
Physical volume     /dev/sdc2
Physical extents    0 to 2018
```

Das LVM-Volume ist auf 16 GB erweitert und kann verwendet werden.

Überprüfen, dass der Zielknoten wiederhergestellt wurde

Überprüfen Sie nach Abschluss des Wiederherstellungsjobs, dass der Zielknoten mit den relevanten Daten wiederhergestellt wurde.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu dem Zielcomputer, den Sie wiederhergestellt haben.
2. Überprüfen Sie, dass der Zielcomputer über alle Daten verfügt, die Sie gesichert haben.

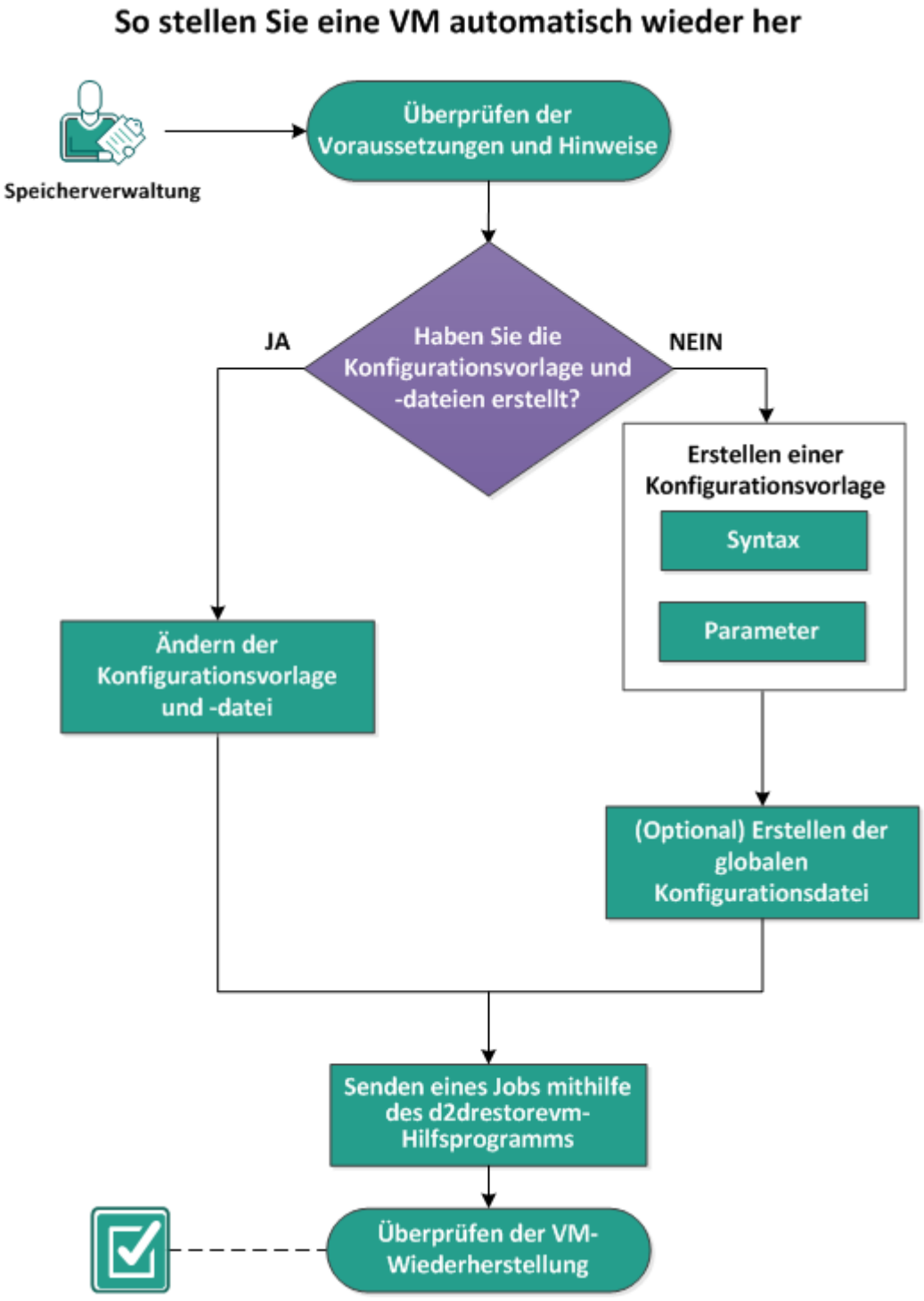
   Der Zielcomputer wurde erfolgreich überprüft.

Die BMR wurde erfolgreich für Linux-Rechner ausgeführt.

So stellen Sie einen virtuellen Rechner automatisch wieder her

Sie können einen virtuellen Rechner (VM) mithilfe des d2drestorevm-Hilfsprogramms über die Befehlszeile des Sicherungsservers wiederherstellen. Das d2drestorevm-Hilfsprogramm automatisiert den Prozess der BMR-Ausführung ohne die Notwendigkeit, die VM über eine Live-CD starten zu müssen.

Die folgende Abbildung veranschaulicht den Vorgang zum Wiederherstellen eines virtuellen Rechners über die Befehlszeile mithilfe des d2drestorevm-Hilfsprogramms:



Führen Sie die folgenden Aufgaben aus, um eine VM automatisch wiederherzustellen:

- Überprüfen der Voraussetzungen und Hinweise (siehe Seite 132)
- Erstellen einer Konfigurationsvorlage (siehe Seite 135)
- (Optional) Erstellen der globalen Konfigurationsdatei (siehe Seite 139)
- Ändern der Konfigurationsvorlage und -datei (siehe Seite 141)
- Senden eines Jobs mithilfe des d2drestorevm-Hilfsprogramms (siehe Seite 141)
- Überprüfen der VM-Wiederherstellung (siehe Seite 142)

Überprüfen der Voraussetzungen und Hinweise

Überprüfen Sie die folgenden Voraussetzungen, bevor Sie die VM wiederherstellen:

- Die folgenden Hypervisor-Versionen werden für BMR mithilfe des d2drestorevm-Hilfsprogramms unterstützt:
  - XenServer 6.0 und höher
  - RHEV 3.0 und höher
  - OVM 3.2
- Die VM-Wiederherstellungsoption kann nur über die Befehlszeile ausgeführt werden. Diese Option ist auf der Benutzeroberfläche nicht verfügbar.
- Sie können die Benutzeroberfläche verwenden, um Jobstatus und Aktivitätsprotokolle zu überwachen. Sie können die Benutzeroberfläche verwenden, um den VM-Wiederherstellungsjob zu unterbrechen, zu löschen und erneut auszuführen. Sie können den VM-Wiederherstellungsjob aber nicht ändern.
- Bevor Sie eine VM wiederherstellen, müssen Sie sie manuell unter Xen, Oracle Virtual Machine (OVM) oder Red hat Enterprise Virtualization (RHEV) einrichten.
- Für Wiederherstellungen auf virtuellen Xen- und OVM-Rechnern muss der NFS-Server auf dem Sicherungsserver installiert sein und ausgeführt werden. Stellen Sie sicher, dass die Firewall den NFS-Dienst nicht blockiert und der Hypervisor über ordnungsgemäßen Zugriff und Berechtigungen für die Verwendung des NFS-Dienstes auf dem Sicherungsserver verfügt.

- Für Wiederherstellungen auf RHEV müssen Version 5.10.0 oder höher des Perl-Interpreter sowie die folgenden Module auf dem Sicherungsserver installiert sein:

  ```
  XML::Simple
  ```

  ```
  URI::Escape
  ```

  ```
  WWW::Curl
  ```

  ```
  File::Copy
  ```

  ```
  File::Temp
  ```

  Die Module können über den Systempaketmanager installiert werden. Sie können auch den Perl-Paketmanager, CPAN, verwenden, um die Module zu installieren.

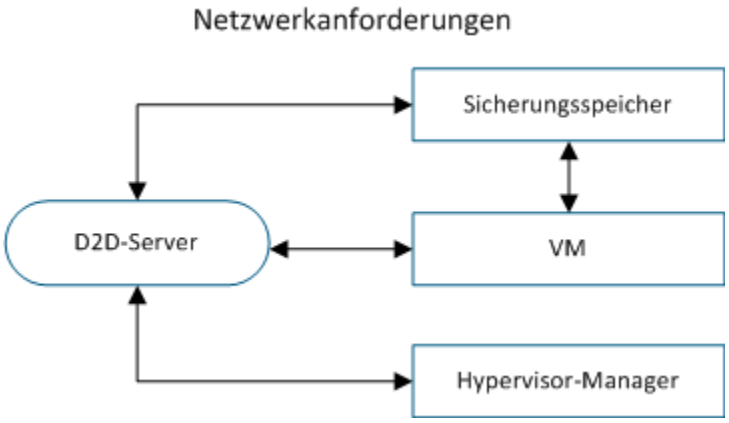
  Beispiel: Installieren von "XML::Simple" mithilfe von CPAN

  ```
  # perl -MCPAN -e "install XML::Simple"
  ```

  Führen Sie den folgenden Befehl aus, um die Installation zu überprüfen:

  ```
  # perldoc -l " XML::Simple"
  ```

- Um eine erfolgreiche VM-Wiederherstellung auszuführen, müssen sowohl der Hypervisor als auch die Ziel-VM über eine gültige Netzwerkverbindung mit dem Sicherungsserver verfügen. Die folgende Abbildung veranschaulicht die Netzwerkvoraussetzungen:



Der Sicherungsserver wird versuchen, automatisch eine virtuelle NIC für die VM zu erkennen und einzurichten. In manchen Fällen wird kein gültiges Netzwerk für die NIC ausgewählt. Mit dem Parameter "vm_network" können Sie ein spezifisches Netzwerk angeben, mit dem die NIC verbunden werden sollte. Beachten Sie folgende Hinweise für unterschiedliche virtuelle Plattformen:

- Unter XenServer wird das Standardnetzwerk nach einer Installation in XenCenter als "Network 0" angezeigt, was nicht dem tatsächlichen Netzwerk entspricht. Alle Netzwerke mit dem Namen "Pool-wide network associated with xxx" werden in XenCenter als "Network 0" angezeigt. Benennen Sie in solchen Fällen das Standardnetzwerk um, und verwenden Sie den neuen Wert für den Parameter "vm_network".
- Wenn der Parameter "vm_network" unter RHEV nicht angegeben ist, hat das standardmäßige RHEV-Netzwerk Priorität.
- Unter OVM wird empfohlen, den Parameter "vm_network" manuell festzulegen, wenn mehr als ein Netzwerk verfügbar ist.

- Wenn die CIFS-Freigabe als Speicherort der Sicherung (Sitzung) verwendet wird, beachten Sie die folgenden Punkte:
  - Verwenden Sie das Zeichen / anstelle von \.
  - Die Parameter "storage_username" und "storage_password" sind erforderlich, um die Anmeldeinformationen für CIFS-Freigaben zu überprüfen.
- Mindestens einer der folgenden Parameter muss angegeben werden, damit d2drestorevm-Hilfsprogramm ordnungsgemäß funktioniert:

  `vm_name`

  `vm_uuid`

  Wenn beide Parameter angegeben werden, müssen sie zum selben virtuellen Rechner gehören. Wenn die Parameter zu unterschiedlichen virtuellen Rechnern gehören, wird ein Fehler zurückgegeben.
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Beachten Sie die folgenden Hinweise, bevor Sie die VM wiederherstellen:

- Es wird empfohlen, die Sitzungen der früheren Version von Arcserve UDP Agent (Linux) oder Arcserve Unified Data Protection Agent for Linux auf den ursprünglichen VMs wiederherzustellen.
- Wenn Sie eine VM in einem XenServer-PV wiederherstellen und die wiederhergestellte VM ein leeres Fenster anzeigt, SSH und andere Dienste jedoch aktiv sind, überprüfen Sie, ob der Parameter "'console='kernel" in den Startargumenten richtig festgelegt ist.
- PV-Sitzungen können nur auf einer PV-Ziel-VM auf XenServer und OVM wiederhergestellt werden.
- Nicht-PV-Sitzungen können auf Nicht-PV-Ziel-VMs wie XenServer HVM, OVM HVM und RHEV wiederhergestellt werden.
- HVMs von RHEL 6-Reihen und ihren Derivaten (RHEL 6, CentOS 6 und Oracle Linux6) können auf PV-VMs wiederhergestellt werden.

Erstellen einer Konfigurationsvorlage

Erstellen Sie eine Konfigurationsdatei, damit der Befehl "d2drestorevm" VMs basierend auf den Parametern, die in dieser Datei angegeben sind, wiederherstellen kann. Die Datei "d2drestorevm" erfasst alle Spezifikationen aus der Datei und führt die Wiederherstellung basierend auf diesen Spezifikationen aus.

Syntax

```
d2drestorevm --createtemplate=[Speicherpfad]
```

Das Hilfsprogramm "d2dutil --encrypt" verschlüsselt das Kennwort und stellt ein verschlüsseltes Kennwort zur Verfügung. Sie müssen dieses Hilfsprogramm für die Verschlüsselung aller Ihrer Kennwörter verwenden. Wenn Sie den Parameter "--pwdfile=pwdfilepath" verwenden, müssen Sie das Kennwort verschlüsseln. Sie können das Hilfsprogramm mit einer der folgenden Methoden einsetzen:

Methode 1

```
echo "string" | d2dutil --encrypt
```

"string" steht für das Kennwort, das Sie angeben.

Methode 2

Tippen Sie den Befehl "d2dutil –encrypt", und geben Sie anschließend Ihr Kennwort an. Wenn Sie die Eingabetaste drücken, wird das Ergebnis auf Ihrem Bildschirm angezeigt. Mit dieser Methode wird das Kennwort, das Sie eingeben, nicht auf dem Bildschirm wiedergegeben.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Erstellen Sie die Konfigurationsvorlage mithilfe des folgenden Befehls:

   ```
   d2drestorevm --createtemplate=[Speicherpfad]
   ```

   [Speicherpfad] steht für den Speicherort, an dem die Konfigurationsvorlage erstellt wird.
3. Öffnen Sie die Konfigurationsvorlage, und aktualisieren Sie die folgenden Parameter:

   job_name

   Gibt den Namen des Wiederherstellungsjobs an.

   vm_type

   Gibt den Typ des Hypervisor an, auf dem Sie die VM wiederherstellen. Die gültigen Hypervisor-Typen sind xen, ovm und rhev.

   vm_server

   Gibt die Adresse des Hypervisor-Servers an. Bei der Adresse kann es sich um den Hostnamen oder die IP-Adresse handeln.

   vm_svr_username

   Gibt den Benutzernamen des Hypervisor an. Für RHEV muss der Benutzername im folgenden Format eingegeben werden:

   ```
   [Benutzername]@[Domäne]
   ```

   Für OVM und Xen muss der Benutzername im folgenden Format eingegeben werden:

   ```
   [Benutzername]
   ```

   vm_svr_password

   Gibt das Kennwort des Hypervisor an. Das Kennwort wird mithilfe des Verschlüsselungshilfsprogramms "d2dutil" verschlüsselt.

vm_name

Gibt den Namen der Ziel-VM an, die im Hypervisor angezeigt wird.

Wichtig! Der Parameter "vm_name" darf keine Sonderzeichen außer Leerzeichen enthalten, und es sollten nur folgende Zeichen verwendet werden: a-z, A-Z, 0-9, - und _.

vm_uuid

Gibt die UUID der Ziel-VM an.

vm_network

(Optional) Gibt den Namen des Netzwerks an, das Sie verwenden möchten. Wenn Sie keinen Netzwerknamen angeben, wird automatisch das Standardnetzwerk ausgewählt.

storage_location

Gibt den Speicherort des Speicherservers der Sitzung an. Der Speicherort kann CIFS oder NFS sein.

storage_username

Gibt den Benutzernamen an, wenn Sie als Speicherort CIFS verwenden.

storage_password

Gibt das Kennwort an, wenn Sie als Speicherort CIFS verwenden. Das Kennwort wird mithilfe des Verschlüsselungshilfsprogramms "d2dutil" verschlüsselt.

encryption_password

Gibt das Verschlüsselungskennwort der Sitzung an. Das Kennwort wird mithilfe des Verschlüsselungshilfsprogramms "d2dutil" verschlüsselt.

source_node

Gibt den Namen des Knotens an, dessen Wiederherstellungspunkt für die Wiederherstellung verwendet wird.

recovery_point

Gibt die Sitzung an, die Sie wiederherstellen möchten. Wiederherstellungssitzungen werden üblicherweise im Format "S00000000X" angegeben, wobei "X" für einen numerischen Wert steht. Wenn Sie die letzte Sitzung wiederherstellen möchten, geben Sie das Schlüsselwort "last" an.

guest_hostname

Gibt den Hostnamen an, den Sie nach der VM-Wiederherstellung angeben möchten.

guest_network

Gibt den Netzwerktyp an, den Sie konfigurieren möchten. Das Netzwerk kann DHCP oder statisch sein.

guest_ip

Gibt die IP-Adresse an, wenn Sie eine statische IP angeben.

guest_netmask

Gibt die Netzwerkmaske an, wenn Sie eine statische IP angeben.

guest_gateway

Gibt die Gateway-Adresse an, wenn Sie eine statische IP angeben.

guest_reboot

(Optional) Gibt an, ob die Ziel-VM nach der VM-Wiederherstellung neu gestartet werden soll. Die Werte sind "yes" (ja) und "no" (nein).

Standard: no

guest_reset_username

(Optional) Gibt an, dass das Kennwort auf den Wert, den Sie im Parameter "guest_reset_password" angeben, zurückgesetzt werden soll.

guest_reset_password

(Optional) Gibt an, dass das Kennwort auf den angegebenen Wert zurückgesetzt werden soll. Das Kennwort wird mithilfe des Verschlüsselungshilfsprogramms "d2dutil" verschlüsselt.

force

Gibt an, ob die VM-Wiederherstellung erzwungen werden soll. Die Werte sind "yes" (ja) und "no" (nein).

Standard: no

4. Speichern und schließen Sie die Konfigurationsvorlage.

Die Konfigurationsvorlage wurde erfolgreich erstellt.

(Optional) Erstellen einer globalen Konfigurationsdatei

Die globale Konfigurationsdatei (vm.cfg) enthält Parameter und Werte für die Speicherorte, an denen die virtuellen Datenträger der VM erstellt werden. Die Werte für Speicherorte werden während der Wiederherstellung automatisch erkannt. Die Datei "vm.cfg" überschreibt die Werte für Speicherorte und andere Parameter. Wenn Sie anstelle des automatisch erkannten Werts Ihren eigenen Speicherort angeben möchten, können Sie die Datei "vm.cfg" verwenden.

Die globale Konfigurationsdatei befindet sich unter folgendem Speicherort:

```
/opt/CA/d2dserver/configfiles/vm.cfg
```

Die folgenden Parameter können in der Datei "vm.cfg" konfiguriert werden:

Allgemeine Parameter

D2D_VM_PORT

Ermöglicht es Ihnen, einen benutzerdefinierten Port für die Kommunikation mit dem Hypervisor-Server anzugeben.

- Unter OVM ist für den Befehl "d2drestorevm" die OVM CLI-Schnittstelle erforderlich, und der Standardport ist 10000.
- Unter XenServer kommuniziert der Befehl "d2drestorevm" mit dem Server mit SSH, und der Standardport ist 22.
- Unter RHEV verwendet der d2drestorevm-Befehl die Representational State Transfer-API (REST), um über HTTPS mit dem Server zu kommunizieren.

OVM-spezifische Parameter

OVM_ISO_REPOSITORY

Ermöglicht es Ihnen, das Repository zum Hochladen der Arcserve UDP Agent (Linux)-Live-CD manuell festzulegen.

OVM_ISO_UPLOAD_SERVER

Ermöglicht es Ihnen, den Repository-Server zum Hochladen der Arcserve UDP Agent (Linux)-Live-CD manuell anzugeben.

OVM_DISK_REPOSITORY

Ermöglicht es Ihnen, für die Erstellung von virtuellen Datenträgern ein spezifisches OVM-Repository zu verwenden.

Hinweis: Das d2drestorevm-Hilfsprogramm verwendet die ID für die OVM-spezifischen Parameter.

RHEV-spezifische Parameter

RHEV_DISK_STORAGE_DOMAIN

Ermöglicht es Ihnen, für die Erstellung von virtuellen Datenträgern eine spezifische XEN-Speicherdomäne zu verwenden. Das d2drestorevm-Hilfsprogramm verwendet den lexikalischen Dateinamen für die RHEV-spezifischen Parameter.

Xen-spezifische Parameter

XEN_DISK_SR

Ermöglicht es Ihnen, für die Erstellung von virtuellen Datenträgern ein spezifisches XEN-Speicher-Repository zu verwenden. Das d2drestorevm-Hilfsprogramm verwendet den lexikalischen Dateinamen für die Xen-spezifischen Parameter.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Sicherungsserver an.
2. Erstellen Sie die globale Konfigurationsdatei, und nennen Sie "vm.cfg".
3. Öffnen Sie die globale Konfigurationsdatei, und aktualisieren Sie die Parameter in der Datei.
4. Speichern und schließen Sie die Datei.
5. Legen Sie die Datei im Ordner "configfiles" ab:

   ```
   /opt/CA/d2dserver/configfiles/vm.cfg
   ```

Die globale Konfigurationsdatei wurde erfolgreich erstellt.

Ändern der Konfigurationsvorlage und -datei

Wenn die Konfigurationsvorlage und die globale Konfigurationsdatei bereits vorhanden sind, können Sie die Dateien ändern und eine andere VM wiederherstellen. Sie müssen nicht jedes Mal, wenn Sie eine VM wiederherstellen, eine neue Konfigurationsvorlage und -datei erstellen. Wenn Sie den Job übergeben, wird auf der Webbenutzeroberfläche ein neuer Job hinzugefügt. Sie können die Aktivitätsprotokolle auf der Webbenutzeroberfläche anzeigen.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Öffnen Sie die Konfigurationsvorlage am Speicherort, an dem Sie die Datei gespeichert haben, und ändern Sie die Parameter nach Ihrem Bedarf.
3. Speichern und schließen Sie die Konfigurationsvorlage.
4. (Optional) Öffnen Sie die globale Konfigurationsdatei vom folgenden Speicherort, und ändern Sie die Parameter nach Ihrem Bedarf:

   ```
   /opt/CA/d2dserver/configfiles/vm.cfg
   ```

5. Speichern und schließen Sie die Konfigurationsdatei.

Die Konfigurationsvorlage und -datei wurden erfolgreich geändert.

Senden eines Jobs mithilfe des d2drestorevm-Hilfsprogramms

Führen Sie den Befehl "d2drestorevm" aus, um die VM wiederherzustellen. Der Befehl überprüft die Ziel-VM und übergibt einen Wiederherstellungsjob. Der Wiederherstellungsjob kann auf der Webbenutzeroberfläche angezeigt werden. Wenn während der Wiederherstellung Anforderungen nicht erfüllt sind, wird ein Fehler zurückgegeben. Sie können das Aktivitätsprotokoll auf der Webbenutzeroberfläche anzeigen.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Übergeben Sie den Wiederherstellungsjob für die VM mithilfe des folgenden Befehls:

   ```
   d2drestorevm --template=cfg_file_path [--wait]
   ```

   Hinweis: Mit dem Schalter "--wait" können Sie nach Abschluss des Wiederherstellungsjobs zur Shell-Umgebung zurückkehren. Wenn der Schalter "--wait" nicht vorhanden ist, kehren Sie nach der Übergabe des Jobs umgehend zur Shell-Umgebung zurück.

Der Wiederherstellungsjob wird übergeben.

Überprüfen der VM-Wiederherstellung

Überprüfen Sie nach Abschluss des Wiederherstellungsjobs, dass der Zielknoten mit den relevanten Daten wiederhergestellt wurde.

Gehen Sie wie folgt vor:

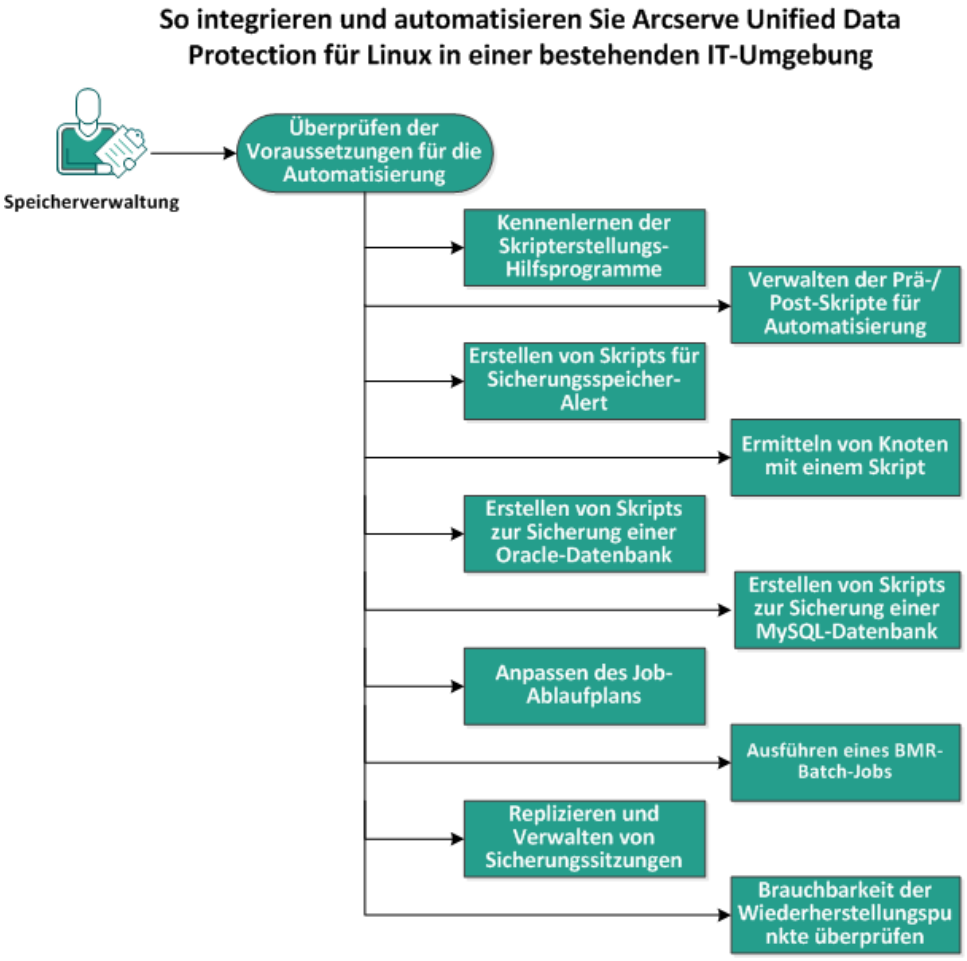
1. Navigieren Sie zur VM, die Sie wiederhergestellt haben.
2. Überprüfen Sie, dass die VM alle Daten enthält, die Sie gesichert haben.

   Die VM wurde erfolgreich überprüft.

So integrieren und automatisieren Sie Arcserve Unified Data Protection Agent for Linux in einer bestehenden IT-Umgebung

Als Storage Manager können Sie Skripte erstellen und die Aufgaben zum Integrieren von Arcserve UDP Agent (Linux) in der bestehenden IT-Umgebung automatisieren. Skripte reduzieren das manuelle Eingreifen und vermindern die Abhängigkeit von der Webbenutzeroberfläche des Sicherungsservers, um eine Aufgabe auszuführen. Arcserve UDP Agent (Linux) stellt darüber hinaus eine Benutzeroberfläche und Hilfsprogramme für die Jobverwaltung, Knotenverwaltung und Aktivitätsprotokollverwaltung bereit.

Folgendes Diagramm zeigt den Vorgang zur Integration und Automatisierung von Arcserve UDP Agent (Linux) mit der vorhandenen IT-Umgebung:


So integrieren und automatisieren Sie Arcserve Unified Data Protection für Linux in einer bestehenden IT-Umgebung
Speicherverwaltung
Überprüfen der Voraussetzungen für die Automatisierung
Kennenlernen der Skripterstellungs-Hilfsprogramme
Verwalten der Prä-/Post-Skripte für Automatisierung
Erstellen von Skripts für Sicherungsspeicher-Alert
Ermitteln von Knoten mit einem Skript
Erstellen von Skripts zur Sicherung einer Oracle-Datenbank
Erstellen von Skripts zur Sicherung einer MySQL-Datenbank
Anpassen des Job-Ablaufplans
Ausführen eines BMR-Batch-Jobs
Replizieren und Verwalten von Sicherungssitzungen
Brauchbarkeit der Wiederherstellungspunkte überprüfen

Gehen Sie wie folgt vor, um Arcserve UDP Agent (Linux) zu automatisieren und zu verwalten:

- Überprüfen der Voraussetzungen für die Automatisierung (siehe Seite 144)
- Kennenlernen der Skripterstellungs-Hilfsprogramme (siehe Seite 145)
- Verwalten der Prä-/Post-Skripte für Automatisierung (siehe Seite 156)
- Erstellen von Skripts für Sicherungsspeicher-Alert (siehe Seite 159)
- Ermitteln von Knoten mit einem Skript (siehe Seite 159)
- Erstellen von Skripten, um die Oracle-Datenbank zu sichern (siehe Seite 161)
- Erstellen von Skripten, um die MySQL-Datenbank zu sichern (siehe Seite 163)
- Anpassen des Job-Ablaufplans (siehe Seite 165)
- Ausführen eines BMR-Batch-Jobs (siehe Seite 166)
- Replizieren und Verwalten von Sicherungssitzungen (siehe Seite 168)
- Überprüfen, ob die Wiederherstellungspunkte verwendet werden können (siehe Seite 171)

Überprüfen der Voraussetzungen für die Automatisierung

Beachten Sie die folgenden Voraussetzungen, bevor Sie Arcserve UDP Agent (Linux) automatisieren und verwalten:

- Sie verfügen über die root-Anmeldeinformationen für den Sicherungsserver.
- Sie verfügen über Kenntnisse hinsichtlich der Linux-Skripterstellung.
- Sie verfügen über ein besseres Verständnis der Arcserve UDP Agent (Linux)-Webschnittstelle.
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Kennenlernen der Skripterstellungs-Hilfsprogramme

Arcserve UDP Agent (Linux) stellt Skripterstellungs-Hilfsprogramme bereit, um Sie beim Erstellen eines Automatisierungsskripts zu unterstützen. Diese Hilfsprogramme sind auf die Skripterstellung ausgelegt, sodass die Ausgabe optimal für Skripte geeignet ist. Die Hilfsprogramme werden verwendet, um Knoten und Jobs zu verwalten, Sicherungsziele zu replizieren und um Aktivitätsprotokolle zu verwalten.

Alle Hilfsprogramme befinden sich im Ordner *bin* am folgenden Speicherort:

```
/opt/CA/d2dserver/bin
```

Das Hilfsprogramm "d2dutil --encrypt" verschlüsselt das Kennwort und stellt ein verschlüsseltes Kennwort zur Verfügung. Sie müssen dieses Hilfsprogramm für die Verschlüsselung aller Ihrer Kennwörter verwenden. Wenn Sie den Parameter "--pwdfile=pwdfilepath" verwenden, müssen Sie das Kennwort verschlüsseln. Sie können das Hilfsprogramm mit einer der folgenden Methoden einsetzen:

Methode 1

```
echo "string" | d2dutil --encrypt
```

"string" steht für das Kennwort, das Sie angeben.

Methode 2

Tippen Sie den Befehl "d2dutil –encrypt", und geben Sie anschließend Ihr Kennwort an. Wenn Sie die Eingabetaste drücken, wird das Ergebnis auf Ihrem Bildschirm angezeigt. Mit dieser Methode wird das Kennwort, das Sie eingeben, nicht auf dem Bildschirm wiedergegeben.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Navigieren Sie mit dem folgenden Befehl zum Ordner "*bin*":

   ```
   # cd/opt/CA/d2dserver/bin
   ```

3. Führen Sie zum Verwalten von Knoten die folgenden Befehle aus:

   `# ./d2dnode`

   Zeigt eine Liste von verfügbaren Befehlen an, um Ihnen dabei zu helfen, alle verknüpften Linux-Knoten zu verwalten. Mithilfe dieses Befehls können Sie Knoten hinzufügen, löschen, ändern und importieren. Sie können Knoten auch unter Verwendung der Anmeldeinformationen ohne root-Berechtigungen hinzufügen.

   Hinweis: Wenn es sich beim Sicherungsserver um einen eigenständigen Linux-Agent handelt, können Sie alle Parameter des d2dnode-Befehls verwenden. Wenn der Sicherungsserver von der UDP-Konsole verwaltet wird, können Sie nur die Parameter list, add, modify und import des d2dnode-Befehls ausführen. Der Knoten auf der UDP-Konsole wird durch die Parameter list, add, modify und import aktualisiert. Beispielsweise werden durch den Befehl ./d2dnode --list alle Linux-Knoten, die zur UDP-Konsole hinzugefügt werden, aufgelistet.

   `# ./d2dnode --list listet alle Knoten auf, die vom Sicherungsserver verwaltet werden.`

   `# ./d2dnode -–add=nodename/ip -–user=username -–password=password -–description=”the description of that node” --attach=jobname --force`

   Fügt dem Sicherungsserver den spezifischen Knoten hinzu. Wenn Sie ein root-Benutzer sind, verwenden Sie diesen Befehl, um Knoten hinzuzufügen.

   Hinweis: Wenn Sie die Portnummer des Knotens ändern, müssen Sie die neue Portnummer im Parameter "--add" wie im folgenden Beispiel veranschaulicht angeben.

   Beispiel: # ./d2dnode -–add=nodename/ip:new_port -–user=username -–password=password -–description=”the description of that node” --attach=jobname --force

   --attach=jobname

   Fügt einen neuen Knoten zu einem vorhandenen Sicherungsjob hinzu.

   --force

   Erzwingt das Hinzufügen des Knotens, auch wenn der Knoten von einem anderen Sicherungsserver verwaltet wird. Wenn Sie den Parameter *force* entfernen, dann wird der Knoten nicht zu diesem Server hinzugefügt, wenn er von einem anderen Sicherungsserver verwaltet wird.

```
# ./d2dnode --add=nodename --user=username --password=password
--rootuser=rootaccount --rootpwd=rootpassword --pwdfile=pwdfilepath
--description=description --attach=jobname –force
```

Fügt dem Sicherungsserver den spezifischen Knoten hinzu. Wenn Sie kein root-Benutzer sind, verwenden Sie diesen Befehl, um Knoten hinzuzufügen.

Hinweis: Wenn Sie die Portnummer des Knotens ändern, müssen Sie die neue Portnummer im Parameter "--add" wie im folgenden Beispiel veranschaulicht angeben.

Beispiel: # ./d2dnode --add=nodename/ip:new_port --user=username --password=password --rootuser=rootaccount --rootpwd=rootpassword --pwdfile=pwdfilepath --description=description --attach=jobname –force

--user=username

Gibt den Benutzernamen des Benutzers ohne root-Berechtigungen an.

--password=password

Gibt das Kennwort des Benutzers ohne root-Berechtigungen an. Wenn der Parameter "--pwdfile=pwdfilepath" angegeben wird, müssen Sie diesen Parameter nicht angeben.

--rootuser=rootaccount

Gibt den Benutzernamen des root-Benutzers an.

--rootpwd=rootpassword

Gibt das Kennwort des root-Benutzers an. Wenn der Parameter "--pwdfile=pwdfilepath" angegeben wird, müssen Sie diesen Parameter nicht angeben.

--pwdfile=pwdfilepath

(Optional) Gibt das Kennwort des Benutzers mit und des Benutzers ohne root-Berechtigungen an. Dies ist ein optionaler Parameter, der verwendet wird, wenn Sie die Kennwörter des Benutzers mit und des Benutzers ohne root-Berechtigungen in separaten Dateien gespeichert haben. Die Kennwortdatei enthält die folgenden Parameter: "--password=password" und "--rootpwd=rootpassword". Für erhöhte Sicherheit muss das Kennwort mithilfe des Hilfsprogramms "d2dutil –encrypt" verschlüsselt werden. Nachdem Sie das Kennwort verschlüsselt haben, ersetzen Sie das alte Kennwort im Parameter "--pwdfile" durch das verschlüsselte Kennwort .

```
# ./d2dnode --node=nodename --attach=jobname
```

Fügt einen angegebenen Knoten zu einem vorhandenen Sicherungsjob hinzu.

```
# ./d2dnode --modify=nodename/ip --user=username --password=newpassword
--description=newdescription
```

Ändert den Benutzernamen, das Kennwort oder die Beschreibung des hinzugefügten Knotens. Wenn Sie ein root-Benutzer sind, verwenden Sie diesen Befehl, um Knoten zu ändern.

```
# ./d2dnode --modify=nodename --user=username --password=newpassword
--rootuser=rootaccount --rootpwd=newrootpassword --pwdfile=pwdfilepath
--description=newdescription
```

Ändert den Benutzernamen, das Kennwort oder die Beschreibung des hinzugefügten Knotens. Wenn Sie kein root-Benutzer sind, verwenden Sie diesen Befehl, um Knoten zu ändern.

--user=username

Gibt den Benutzernamen des Benutzers ohne root-Berechtigungen an.

--password=newpassword

Gibt das neue Kennwort des Benutzers ohne root-Berechtigungen an.

--rootuser=rootaccount

Gibt den Benutzernamen des root-Benutzers an.

--rootpwd=newrootpassword

Gibt das neue Kennwort des root-Benutzers an.

--pwdfile=pwdfilepath

(Optional) Gibt das Kennwort des Benutzers mit und des Benutzers ohne root-Berechtigungen an. Dies ist ein optionaler Parameter, der verwendet wird, wenn Sie die Kennwörter des Benutzers mit und des Benutzers ohne root-Berechtigungen in separaten Dateien gespeichert haben. Die Kennwortdatei enthält die folgenden Parameter: "--password=newpassword" und "--rootpwd=newrootpassword".

```
# ./d2dnode --delete=nodename1,nodename2,nodename3
```

Löscht die angegebenen Knoten vom Sicherungsserver. Um mehrere Knoten zu löschen, verwenden Sie Kommas (,) als Trennzeichen.

```
# ./d2dnode --import=network --help
```

Importiert Knoten aus dem Netzwerk. Wenn Sie Knoten importieren, können Sie folgende Optionen konfigurieren:

--netlist

Gibt die Liste der IPv4-Adressen an. Bei Mehrfachangaben sollten die Einträge in der Liste durch Kommas voneinander abgetrennt werden.

Beispiel

192.168.1.100: Importiert den Knoten, dessen IP-Adresse 192.168.1.100 lautet

192.168.1.100-150: Importiert alle Knoten im Bereich zwischen 192.168.1.100 und 192.168.100.150

192.168.1.100-: Importiert alle Knoten im Bereich zwischen 192.168.1.100 und 192.168.1.254. In diesem Fall müssen Sie den Endbereich nicht angeben.

192.168.1.100-150,192.168.100.200-250: Importiert mehrere Knoten aus zwei unterschiedlichen Bereichen. Der Bereich ist 192.168.1.100 bis 192.168.1.150, der zweite 192.168.100.200 bis 192.168.100.250. Die Eingaben werden jeweils durch Kommas voneinander abgetrennt.

--joblist

Gibt die Liste der Jobnamen an. Jobnamen dürfen keine Kommas enthalten. Wenn ein Knoten erfolgreich importiert wurde, wird er zum Job hinzugefügt. Bei mehreren Jobs sollten die Einträge in der Liste durch Kommas voneinander abgetrennt werden.

Beispiel: --joblist=jobA,jobB,jobC

In diesem Beispiel sind die einzelnen Jobeinträge durch Kommas voneinander abgetrennt.

Hinweis: Diese Option wird nur von der eigenständigen Version von Arcserve UDP Agent (Linux) unterstützt.

--user

Gibt den Benutzernamen für das Importieren und Hinzufügen der Knoten an.

--password

Gibt das Kennwort für das Importieren und Hinzufügen der Knoten an.

--rootuser

Gibt den Benutzernamen des root-Benutzers an. Wenn ein Benutzer ohne root-Berechtigungen hinzugefügt wird, verwenden Sie diesen Parameter, um die Anmeldeinformationen des root-Benutzers anzugeben.

--rootpwd

Gibt das Kennwort des root-Benutzers an. Wenn ein Benutzer ohne root-Berechtigungen hinzugefügt wird, verwenden Sie diesen Parameter, um die Anmeldeinformationen des root-Benutzers anzugeben.

--pwdfile

(Optional) Gibt das Kennwort des Benutzers mit und des Benutzers ohne root-Berechtigungen an. Dies ist ein optionaler Parameter, der verwendet wird, wenn Sie die Kennwörter des Benutzers mit und des Benutzers ohne root-Berechtigungen in separaten Dateien gespeichert haben. Die Kennwortdatei enthält die folgenden Parameter: "--password=newpassword" und "--rootpwd=newrootpassword".

--prefix

Gibt das Präfix für einen Hostnamen an. Verwenden Sie diesen Parameter, um nach Knoten zu filtern, deren Hostname dieses Präfix enthält.

--blacklistfile

Gibt eine Datei an, die eine Liste von Knoten-Hostnamen enthält, die Sie nicht zum Sicherungsserver hinzufügen möchten. Sie müssen in der Datei einen Knoten pro Zeile angeben.

--force

Erzwingt das Hinzufügen des Knotens, auch wenn der Knoten von einem anderen Sicherungsserver verwaltet wird. Wenn Sie den Parameter *force* entfernen, dann wird der Knoten nicht zu diesem Server hinzugefügt, wenn er von einem anderen Sicherungsserver verwaltet wird.

--verbose

Zeigt weitere Informationen zum Knotenimportprozess an. Verwenden Sie diesen Parameter für Debugging oder die Erstellung von Automatisierungsskripten.

--help

Zeigt den Hilfe-Bildschirm an.

Hinweise:

- Die Importfunktion verwendet den SSH-Server, um zu ermitteln, ob es sich bei einem Knoten um einen Linux-Knoten handelt. Wenn Ihr SSH-Server einen nicht standardmäßigen Port verwendet, konfigurieren Sie den Server für die Verwendung des nicht standardmäßigen Ports. Weitere Informationen zum Konfigurieren der Nummer des SSH-Ports finden Sie unter Ändern der SSH-Portnummer des Sicherungsservers.
- Wenn kein Kennwort angegeben wird, wird die Authentifizierungsmethode mit SSH-Schlüsseln verwendet.

4. Führen Sie zum Verwalten von Jobs die folgenden Befehle aus:

```
# ./d2djob
```

Zeigt eine Liste von Befehlen an, die Sie beim Verwalten von Jobs unterstützen. Mithilfe dieses Befehls können Sie Jobs ausführen, abbrechen und löschen.

```
# ./d2djob -—delete=jobname
```

Löscht den angegebenen Job aus der Registerkarte "Jobstatus".

```
# ./d2djob -—run=jobname -—jobtype=1 -—wait
```

Führt den angegebenen Job aus. Der Parameter "--jobtype" ist optional. Der Befehl "d2djob" identifiziert den Jobtyp durch den Jobnamen, den Sie angeben, automatisch. Wenn der Befehl einen Wiederherstellungsjob identifiziert, wird der Wiederherstellungsjob gestartet. Wenn der Befehl einen Sicherungsjob identifiziert und Sie keinen Wert für den Parameter "--jobtype" angeben, wird ein Zuwachssicherungsjob gestartet. Die Zuwachssicherung ist der standardmäßige Jobtyp.

Die Werte für die Angabe des Jobtyps eines Sicherungsjobs sind 0, 1 und 2, wobei 0 für eine vollständige Sicherung, 1 für eine Zuwachssicherung und 2 für eine Überprüfungssicherung steht.

```
# ./d2djob -—cancel=jobname -—wait
```

Bricht einen Job ab, der in Bearbeitung ist.

Wenn Sie -"-wait" in den Befehl aufnehmen, wird der Jobstatus angezeigt, nachdem der Job abgebrochen wurde. Wenn Sie "--wait" nicht in den Befehl aufnehmen, wird der Jobstatus sofort angezeigt, nachdem die Abbruchanforderung übergeben wurde.

```
# ./d2djob --newrestore=restoreJobName --target=macaddress/ipaddress
--hostname=hostname --network=dhcp/staticip --staticip=ipaddress
--subnet=subnetMask --gateway=gateway --runnow --wait
```

Führt einen Wiederherstellungsjob, der auf einem vorhandenen Wiederherstellungsjob basiert, für einen neuen Zielcomputer aus. Dieser Befehl ermöglicht es Ihnen, die gleichen Wiederherstellungseinstellungen wie der vorhandene Wiederherstellungsjob zu verwenden, und nur die Zielcomputerdetails sind anders. Wenn Sie diesen Befehl verwenden, müssen Sie nicht mehrere Wiederherstellungsjobs für verschiedene Zielcomputer erstellen.

Sie müssen einen Wert für *--newrestore*, *--target*, *--hostname* und *--network* angeben.

Wenn der Wert für *--network* ist "staticip", dann müssen Sie einen Wert für *--staticip*, *--subnet* und *--gateway* angeben. Wenn der Wert für *--network* ist "dhcp", dann müssen Sie keinen Wert für *--staticip, --subnet* und *--gateway* angeben.

Wenn Sie "--runnow" in den Befehl aufnehmen, wird der Job sofort ausgeführt, nachdem Sie den Job, unabhängig vom Jobablaufplan, übergeben.

Wenn Sie den Parameter "--wait" in den Befehl einschließen, wird die Statusmeldung nach dem Abschluss des Jobs angezeigt. Wenn Sie "--wait" nicht in den Befehl aufnehmen, wird die Statusmeldung sofort angezeigt, nachdem der Job übergeben wurde.

```
# ./d2djob <--export=jobname1,jobname2,jobname3> <--file=filepath>
```

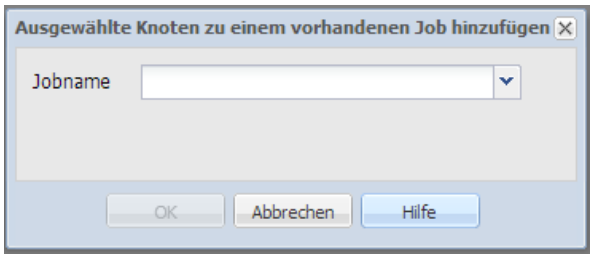
Exportiert mehrere Jobs vom Sicherungsserver in eine Datei. Wenn Sie in mehreren Sicherungsservern ähnliche Sicherungskonfigurationen verwenden möchten, können Sie die Sicherungsjobs in eine Datei exportieren und diese Datei in andere Sicherungsserver importieren.

Hinweis: Wenn der Linux-Sicherungsserver von der Arcserve UDP-Konsole verwaltet wird, wird die Exportfunktion nicht unterstützt.

```
# ./d2djob <--import=filepath>
```

Importiert die Datei, die die Sicherungsjobinformationen enthält, in einen Sicherungsserver. Sie können die Datei auch in Arcserve UDP importieren, wenn der Sicherungsserver von Arcserve UDP verwaltet wird.

Wenn der Sicherungsjob zu einem Sicherungsserver importiert wird, können Sie den Job in folgendem Dialogfeld auswählen:



Sie können auch das folgende Befehlszeilenhilfsprogramm verwenden, um Knoten zu diesem Job hinzuzufügen:

```
./d2dnode –attach=jobname
```

5. Führen Sie folgende Befehle aus, um die Konfigurationsdatei der Wiederherstellungspunkte zu erstellen oder zu aktualisieren. Arcserve UDP Agent (Linux) verwendet die Konfigurationsdatei, um die Wiederherstellungspunkte in der Benutzeroberfläche zu verwalten und anzuzeigen.

```
# ./d2drp
```

Erstellt oder aktualisiert die Konfigurationsdateien der Wiederherstellungspunkte, die auf den Details der Wiederherstellungspunkte basieren. Mithilfe dieses Befehls können Sie die Konfigurationsdateien erstellen oder aktualisieren.

```
# ./d2drp --build ––storagepath=/backupdestination –-node=node_name
```

Überprüft alle Wiederherstellungspunkte, die zu *node_name* gehören, und aktualisiert alle Konfigurationsdateien der Wiederherstellungspunkte. Wenn die Konfigurationsdateien der Wiederherstellungspunkte nicht vorhanden sind, dann erstellt dieser Befehl die Dateien automatisch. Durch den Parameter "--build" werden die Konfigurationsdateien von Wiederherstellungspunkten erstellt.

```
# ./d2drp --build –-storagepath=/backupdestination –-node=node_name
–-rp=recovery_point
```

Überprüft den angegebenen Sitzungsnamen und aktualisiert alle Konfigurationsdateien der Wiederherstellungspunkte. Wenn die Konfigurationsdateien der Wiederherstellungspunkte nicht vorhanden sind, dann erstellt dieser Befehl die Dateien automatisch. Geben Sie das Schlüsselwort "last" an, damit der Parameter "--rp" den aktuellsten Wiederherstellungspunkt abruft.

```
# ./d2drp  --show --storagepath=path --node=nodeName --rp=recovery_point
--user=username --password=password
```

Zeigt Systeminformationen für den angegebenen Wiederherstellungspunkt an.

--rp=recovery_point

Gibt den Wiederherstellungspunkt an, auf den Sie zugreifen möchten. Geben Sie das Schlüsselwort "last" an, damit der aktuellste Wiederherstellungspunkt abgerufen wird.

--user=username

Gibt den Benutzernamen an, mit dem auf den Speicherort oder das Sicherungsziel zugegriffen werden soll.

--password=password

Gibt das Kennwort an, mit dem auf den Speicherort oder das Sicherungsziel zugegriffen werden soll.

Hinweis: Für den Parameter "--build" unterstützt "d2drp" keine NFS- oder CIFS-Freigaben. Wenn Sie die NFS-Freigabe oder die CIFS-Freigabe verwenden möchten, müssen Sie zuerst die Freigabe auf den lokalen Host laden und anschließend den Bereitstellungspunkt als "storagepath" verwenden.

6. Führen Sie den folgenden Befehl aus, um den Sicherungsserver bei Arcserve UDP zu registrieren. Wenn Sie den Sicherungsserver bei Arcserve UDP registrieren, können Sie ihn über Arcserve UDP verwalten. Sie können auch Knoten und Jobs, die zuvor vom Sicherungsserver verwaltet wurden, in Arcserve UDP importieren.

   ```
   # ./d2dreg <--reg=servername> <--user=username> <--port=port>
   <--protocol=http/https> [--password=password]
   ```

   Registriert den Sicherungsserver bei Arcserve UDP, wodurch der Sicherungsserver über die Arcserve UDP-Konsole verwaltet werden kann.

   Hinweis: Der d2dreg-Befehl verwendet den Hostnamen des Sicherungsservers, um den Server zu identifizieren. Wenn die Arcserve UDP-Konsole mithilfe des Hostnamens keine Verbindung mit dem Sicherungsserver aufbauen kann, ändern Sie den Hostnamen im Dialogfeld **Knoten aktualisieren** in die IP-Adresse um.

7. Führen Sie die folgenden Befehle aus, um Aktivitätsprotokolle zu verwalten:

   ```
   # ./d2dlog
   ```

   Zeigt das Format an, das Ihnen dabei hilft, die Aktivitätsprotokolle für die angegebene Job-ID im angegebenen Format abzurufen.

   ```
   # ./d2dlog -—show=jobid -—format=text/html
   ```

   Zeigt das Aktivitätsprotokoll des angegebenen Jobs an. Der Formatwert ist optional, weil der Standardwert Text ist.

8. Führen Sie die folgenden Befehle aus, um den Jobverlauf zu verwalten:

   ```
   # ./d2djobhistory
   ```

   Zeigt den Jobverlauf basierend auf den von Ihnen angegebenen Filtern an. Sie können den Jobverlauf nach Tagen, Wochen, Monaten, Anfangs- und Enddatum filtern.

```
# ./d2djobhistory --day=n --headers=column_name1,column_name2,...column_name_n
--width=width_value --format=column/csv/html
```

Zeigt den aktuellen Jobverlauf basierend auf den angegebenen Tagen an.

--headers=column_name1,column_name2,...column_name_n

(Optional) Gibt die Spalten an, die im Jobverlauf angezeigt werden sollen. Dies ist ein optionaler Parameter. Die vordefinierten Spalten sind ServerName, TargetName, JobName, JobID, JobType, DestinationLocation, EncryptionAlgoName, CompressLevel, ExecuteTime, FinishTime, Throughput, WriteThroughput, WriteData, ProcessedData und Status.

--width=width_value

(Optional) Gibt die Anzahl von Zeichen an, die jeweils pro Spalte angezeigt werden sollen. Dies ist ein optionaler Parameter. Jede Spalte hat ihre eigene Standardbreite. Sie können den Breitenwert der einzelnen Spalte aktualisieren, wobei Breitenwerte durch Kommas (,) voneinander getrennt werden.

--format=column/csv/html

Gibt das Anzeigeformat des Jobverlaufs an. Die verfügbaren Formate sind column, csv und html. Sie können nur ein einziges Format angeben.

```
# ./d2djobhistory --week=n
--headers=column_name1,column_name2,...column_name_n --width=width_value
--format=column/csv/html
```

Zeigt den aktuellen Jobverlauf basierend auf den angegebenen Wochen an.

```
# ./d2djobhistory --month=n
--headers=column_name1,column_name2,...column_name_n --width=width_value
--format=column/csv/html
```

Zeigt den aktuellen Jobverlauf basierend auf den angegebenen Monaten an.

```
# ./d2djobhistory --starttime=yyyymmdd --endtime=yyyymmdd
--headers=column_name1,column_name2,...column_name_n --width=width_value
--format=column/csv/html
```

Zeigt den aktuellen Jobverlauf basierend auf den angegebenen Anfangs- und Enddaten an.

Die Skripterstellungs-Hilfsprogramme wurden verwendet, um erfolgreich Knoten, Jobs und Aktivitätsprotokolle zu verwalten.

Verwalten der Prä-/Post-Skripte für Automatisierung

Mit Prä-/Post-Skripts können Sie Ihre eigene Geschäftslogik in bestimmten Phasen eines in Bearbeitung befindlichen Jobs ausführen. Sie können in **Einstellungen vor/nach dem Skript** im **Sicherungsassistenten** und **Wiederherstellungsassistenten** in der Konsole angeben, wann Ihre Skripte ausgeführt werden sollen. Die Skripts können je nach Einstellung auf dem Sicherungsserver ausgeführt werden.

Das Verwalten von Prä-/Post-Skripts ist ein zweiteiliger Vorgang, der das Erstellen des Prä-/Post-Skripts und das Einfügen des Skripts in den "prepost"-Ordners umfasst.

Erstellen von Prä-/Post-Skripts

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Erstellen Sie eine Skriptdatei, indem Sie die Umgebungsvariablen in Ihrer bevorzugten Skripterstellungssprache verwenden.

   Umgebungsvariablen des Prä-/Post-Skripts

   Verwenden Sie die folgenden Umgebungsvariablen, um Ihr Skript zu erstellen:

   D2D_JOBNAME

   Gibt den Namen des Jobs an.

   D2D_JOBID

   Gibt die Job-ID an. Die Job-ID ist eine Nummer, die für den Job vergeben wird, wenn Sie den Job ausführen. Wenn Sie den gleichen Job erneut ausführen, erhalten Sie eine neue Jobnummer.

   D2D_TARGETNODE

   Identifiziert den Knoten, der gesichert oder wiederhergestellt wird.

   D2D_JOBTYPE

   Identifiziert den Typ des ausgeführten Jobs. Die folgenden Werte identifizieren die D2D_JOBTYPE-Variable:

   backup.full

   Identifiziert den Job als eine vollständige Sicherung.

   backup.incremental

   Identifiziert den Job als eine Zuwachssicherung.

   backup.verify

   Identifiziert den Job als eine Überprüfungssicherung.

restore.bmr

Identifiziert den Job als eine Bare-Metal-Recovery (BMR). Dies ist ein Wiederherstellungsjob.

restore.file

Identifiziert den Job als eine Wiederherstellung auf Dateiebene. Dies ist ein Wiederherstellungsjob.

D2D_SESSIONLOCATION

Identifiziert den Speicherort, an dem die Wiederherstellungspunkte gespeichert sind.

D2D_PREPOST_OUTPUT

Identifiziert eine Temp-Datei. Der Inhalt der Anfangszeile der Temp-Datei wird im Aktivitätsprotokoll angezeigt.

D2D_JOBSTAGE

Gibt die Phase des Jobs an. Die folgenden Werte identifizieren die D2D_JOBSTAGE-Variable:

pre-job-server

Identifiziert das Skript, das auf dem Sicherungsserver ausgeführt wird, bevor der Job startet.

post-job-server

Identifiziert das Skript, das auf dem Sicherungsserver ausgeführt wird, nachdem der Job abgeschlossen ist.

pre-job-target

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, bevor der Job startet.

post-job-target

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, nachdem der Job abgeschlossen ist.

pre-snapshot

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, bevor der Snapshot erfasst wird.

post-snapshot

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, nachdem der Snapshot erfasst wird.

D2D_TARGETVOLUME

Identifiziert das Volume, das während eines Sicherungsjobs gesichert wird. Diese Variable ist anwendbar für Prä-/Post-Snapshot-Skripts für einen Sicherungsjob.

D2D_JOBRESULT

Identifiziert das Ergebnis für ein Post-Job-Skript. Die folgenden Werte identifizieren die D2D_JOBRESULT-Variable:

success

Identifiziert das Ergebnis als erfolgreich.

fail

Identifiziert das Ergebnis als nicht erfolgreich.

D2DSVR_HOME

Identifiziert den Ordner, in dem der Sicherungsserver installiert ist. Diese Variable ist anwendbar für die Skripts, die auf dem Sicherungsserver ausgeführt werden.

Das Skript ist erstellt.

Hinweis: Bei allen Skripten zeigt der Rückgabewert Null eine erfolgreiche Erstellung an, und ein Rückgabewert, der ungleich Null ist, weist auf einen Fehler hin.

Einfügen des Skripts in den Ordner "Prepost" und Überprüfung des Skripts

Alle Prä-/Post-Skripts für einen Sicherungsserver werden zentral vom Ordner "prepost" am folgenden Speicherort verwaltet:

```
/opt/CA/d2dserver/usr/prepost
```

Gehen Sie wie folgt vor:

1. Fügen Sie die Datei in folgenden Speicherort des Sicherungsservers ein:

   ```
   /opt/CA/d2dserver/usr/prepost
   ```

2. Geben Sie der Skriptdatei Ausführungsberechtigungen.
3. Melden Sie sich bei der Arcserve UDP Agent (Linux)-Webbenutzeroberfläche an.
4. Öffnen Sie den **Sicherungsassistenten** oder **Wiederherstellungsassistenten**, und navigieren Sie zur Registerkarte **Erweitert**.
5. Wählen Sie die Skriptdatei in der Drop-down-Liste **Einstellungen vor/nach dem Skript** aus, und übergeben Sie den Job.
6. Klicken Sie auf "**Aktivitätsprotokoll**", und stellen Sie sicher, dass das Skript für den angegebenen Sicherungsjob ausgeführt wird.

   Das Skript wird ausgeführt.

Die Prä-/Post-Skripte wurden erfolgreich erstellt und befinden sich im Ordner "prepost".

Erstellen von Skripts für Sicherungsspeicher-Alert

Erstellen Sie das Skript für Sicherungsspeicher-Alert, sodass Sie das Skript ausführen können, wenn Ihr Speicherplatz für die Sicherung unter dem angegebenen Wert liegt. Wenn Sie einen Sicherungsspeicherort in der Benutzeroberfläche hinzufügen, dann können Sie das Kontrollkästchen für das Senden eines Alerts auswählen. Wenn Sie das Kontrollkästchen aktivieren, überwacht Arcserve UDP Agent (Linux) alle 15 Minuten den verfügbaren Speicherplatz. Jedes Mal, wenn der Speicherplatz unter dem angegebenen Wert liegt, führt Arcserve UDP Agent (Linux) das Skript *backup_storage_alert.sh* aus. Sie können das Skript *backup_storage_alert.sh* konfigurieren, um eine beliebige Aufgabe für Sie auszuführen, wenn der Sicherungsspeicherplatz weniger ist.

Beispiel 1: Sie können das Skript so konfigurieren, dass Ihnen automatisch ein E-Mail-Alert gesendet wird, der Sie auf den verringerten Speicherplatz hinweist.

Beispiel 2: Sie können das Skript so konfigurieren, dass einige Daten automatisch aus dem Sicherungsspeicherplatz gelöscht werden, wenn der Speicherplatz unter dem angegebenen Wert liegt.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Erstellen Sie das Skript *backup_storage_alert.sh* mithilfe der folgenden Variablen:

   backupstoragename

   Definiert den Namen des Sicherungsspeicherorts. Zum Beispiel: "NFS" oder "CIFS".

   freesize

   Definiert den verfügbaren freien Speicherplatz im Sicherungsspeicherort.
3. Fügen Sie das Skript in folgenden Speicherort ein:

   `/opt/CA/d2dserver/usr/alert/backup_storage_alert.sh`

Das Skript "backup_storage_alert.sh" ist erstellt.

Ermitteln von Knoten mit einem Skript

Arcserve UDP Agent (Linux) ermöglicht es Ihnen, ein Skript auszuführen, das Knoten in Ihrem Netzwerk ermittelt. Sie können ein Skript schreiben, um Knoten in Ihrem Netzwerk zu ermitteln, und das Skript anschließend im Ordner *Discovery* einfügen.

Sie können die Einstellung für das Knoten-Discovery in der Web-Benutzeroberfläche konfigurieren und die Häufigkeit der Skriptausführung festlegen. Im Skript können Sie die Hilfsprogramme angeben, um Knoten in Ihrem Netzwerk zu ermitteln. Nachdem das Skript einen Knoten ermittelt hat, verwenden Sie den Befehl "*d2dnode*", um diesen Knoten Arcserve UDP Agent (Linux) hinzuzufügen. Bei jeder Ausführung des Skripts wird ein Aktivitätsprotokoll erstellt.

Hinweis: Bei allen Skripten zeigt der Rückgabewert von Null eine erfolgreiche Erstellung an, und ein Rückgabewert, der ungleich Null ist, weist auf einen Fehler hin.

Wenn Sie in Bezug auf das Knoten-Discovery-Skript Informationen in das Aktivitätsprotokoll aufnehmen möchten, können Sie die folgende spezielle Umgebungsvariable verwenden:

```
echo "print something into activity log" > "$D2D_DISCOVER_OUTPUT"
```

Ein Beispielskript ist im Ordner "*discovery*" am folgenden Speicherort gespeichert, mit dem die Linux-Knoten in einem Sub-Netzwerk ermittelt werden können.

```
/opt/CA/d2dserver/examples/discovery
```

Sie können das Beispielskript an den folgenden Speicherort kopieren und das Skript an Ihre Anforderung anpassen:

```
/opt/CA/d2dserver/usr/discovery
```

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Erstellen Sie ein Knoten-Discovery-Skript, und speichern Sie das Skript im Ordner "*discovery*" an folgendem Speicherort:

   ```
   /opt/CA/d2dserver/usr/discovery
   ```
3. Geben Sie der Skriptdatei die notwendigen Ausführungsberechtigungen.
4. Melden Sie sich bei der Webschnittstelle an.
5. Konfigurieren Sie die Knoten-Discovery-Einstellungen im Menü "Knoten", um das Skript auszuführen.
6. Klicken Sie auf "Aktivitätsprotokoll", und überprüfen Sie, dass das Skript ausgeführt wird.

   Das Aktivitätsprotokoll zeigt eine Liste aller erkannten Knoten an.

Knoten wurden mithilfe des Skripts erfolgreich erkannt.

Erstellen von Skripten, um die Oracle-Datenbank zu sichern

Sie können Skripte erstellen, die Sie verwenden, um Ihre Oracle-Datenbank zu sichern. Sie müssen Ihre Datenbank nicht anhalten, um eine Sicherung auszuführen. Stellen Sie sicher, dass sich die Datenbank im Archivprotokollmodus befindet. Wenn sie sich nicht im Archivprotokollmodus befindet, setzen Sie die Datenbank in den Archivprotokollmodus, bevor Sie sie sichern. Sie erstellen die folgenden zwei Skripte, um eine Oracle-Datenbank zu sichern:

- **pre-db-backup-mode.sh** - Dieses Skript bereitet die gesamte Datenbank vor und behält sie Sicherungsmodus.
- **post-db-backup-mode.sh** - Dieses Skript entfernt die Datenbank aus dem Sicherungsmodus.

Im Sicherungsassistenten können Sie unter Einstellungen für Prä-/Post-Skripts die Skripte angeben, die auf den Knoten der Oracle-Datenbank ausgeführt werden sollen.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Erstellen Sie das Skript *pre-db-backup-mode.sh*, indem Sie folgenden Code verwenden:

```
#!/bin/bash

orauser="oracle"

orasid="orcl"

su - ${orauser}   << BOF 2>&1

export ORACLE_SID=$orasid

sqlplus /nolog << EOF 2>&1

connect / as sysdba

alter database begin backup;

exit;

EOF

BOF
```

Hinweis: Geben Sie den Wert für die Variablen *orauser* und *orasid* so an, wie sie in Ihrer Oracle-Datenbank definiert sind.

3. Erstellen Sie das Skript *post-db-backup-mode.sh*, indem Sie folgenden Code verwenden:

```
#!/bin/bash

orauser="oracle"

orasid="orcl"

su - ${orauser}   << BOF 2>&1

export ORACLE_SID=$orasid

sqlplus /nolog << EOF 2>&1

connect / as sysdba

alter database end backup;

exit;

EOF

BOF
```

   Hinweis: Geben Sie den Wert für die Variablen *orauser* und *orasid* so an, wie sie in Ihrer Oracle-Datenbank definiert sind.

4. Geben Sie beiden Skripten Ausführungsberechtigungen.
5. Fügen Sie beide Skripte am folgenden Speicherort ein:

   ```
   /opt/CA/d2dserver/usr/prepost/
   ```

6. Melden Sie sich bei der Arcserve UDP Agent (Linux)-Webbenutzeroberfläche an.
7. Öffnen Sie den Sicherungsassistenten, und navigieren Sie zur Registerkarte Erweitert.
8. Wählen Sie in der Option Einstellungen für Prä-/Post-Skripts die Skriptdatei *pre-db-backup-mode.sh* in der Drop-down-Liste Vor Aufnehmen des Snapshot aus.
9. Wählen Sie in der Option Einstellungen für Prä-/Post-Skripts die Skriptdatei *post-db-backup-mode.sh* in der Drop-down-Liste Nach Aufnehmen des Snapshot aus.
10. Stellen Sie den Sicherungsjob in die Warteschlange.

    Der Sicherungsjob wird übergeben.

Die Skripte werden erstellt, um die Oracle-Datenbank zu sichern.

Hinweis: Arcserve UDP Agent (Linux) unterstützt Snapshots auf Volume-Ebene. Um die Datenkonsistenz zu sichern, müssen sich alle Datendateien der Datenbank auf einem Volume befinden.

Um die Oracle-Datenbank wiederherzustellen, lesen Sie den Abschnitt So stellen Sie eine Oracle-Datenbank mithilfe von Arcserve UDP Agent (Linux) wieder her (siehe Seite 211).

Erstellen von Skripten, um die MySQL-Datenbank zu sichern

Sie können Skripte erstellen, die Sie verwenden, um Ihre MySQL-Datenbank zu sichern. Sie müssen Ihre Datenbank nicht anhalten, um eine Sicherung auszuführen. Sie erstellen die folgenden zwei Skripte, um eine MySQL-Datenbank zu sichern:

- **pre-db-backup-mode.sh** - Dieses Skript schließt alle offenen Tabellen, und es sperrt alle Tabellen für alle Datenbanken mit einer globalen Lesesperre.
- **post-db-backup-mode.sh** - Dieses Skript hebt alle Sperren auf.

Im Sicherungsassistenten können Sie unter Einstellungen für Prä-/Post-Skripts die Skripte angeben, die auf den Knoten der MySQL-Datenbank ausgeführt werden sollen.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Erstellen Sie das Skript *pre-db-backup-mode.sh*, indem Sie folgenden Code verwenden:

```
#!/bin/bash

dbuser=root

dbpwd=rootpwd

lock_mysqldb(){

  (

    echo "flush tables with read lock;"

    sleep 5

  ) | mysql -u$dbuser -p$dbpwd ${ARGUMENTS}

}

lock_mysqldb &

PID="/tmp/mysql-plock.$!"

touch ${PID}
```

Hinweis: Geben Sie den Wert für die Variablen *dbuser* und *dbpwd* an, wie in Ihrer MySQL-Datenbank definiert.

3. Erstellen Sie das Skript *post-db-backup-mode.sh*, indem Sie folgenden Code verwenden:

```
#!/bin/bash

killcids(){

pid="$1"

cids=`ps -ef|grep ${pid}|awk '{if('$pid'==$3){print $2}}'`

for cid in ${cids}

do

  echo ${cid}

  kill -TERM ${cid}

done

echo -e "\n"

}

mysql_lock_pid=`ls /tmp/mysql-plock.* | awk -F . '{print $2}'`

[ "$mysql_lock_pid" != "" ] && killcids ${mysql_lock_pid}

rm -fr /tmp/mysql-plock.*
```

4. Geben Sie beiden Skripten Ausführungsberechtigungen.
5. Fügen Sie die beiden Skripte am folgenden Speicherort ein:

   ```
   /opt/CA/d2dserver/usr/prepost/
   ```

6. Melden Sie sich bei der Arcserve UDP Agent (Linux)-Webbenutzeroberfläche an.
7. Öffnen Sie den Sicherungsassistenten, und navigieren Sie zur Registerkarte Erweitert.
8. Wählen Sie in der Option Einstellungen für Prä-/Post-Skripts die Skriptdatei *pre-db-backup-mode.sh* in der Drop-down-Liste Vor Aufnehmen des Snapshot aus.
9. Wählen Sie in der Option Einstellungen für Prä-/Post-Skripts die Skriptdatei *post-db-backup-mode.sh* in der Drop-down-Liste Nach Aufnehmen des Snapshot aus.
10. Stellen Sie den Sicherungsjob in die Warteschlange.

    Der Sicherungsjob wird übergeben.

Die Skripte werden erstellt, um die MySQL-Datenbank zu sichern.

Hinweis: Arcserve UDP Agent (Linux) unterstützt Snapshots auf Volume-Ebene. Um die Datenkonsistenz zu sichern, müssen sich alle Datendateien der Datenbank auf einem Volume befinden.

Anpassen des Job-Ablaufplans

Arcserve UDP Agent (Linux) ermöglicht es Ihnen, Ihren eigenen Ablaufplan mithilfe eines Skripts für die Jobausführung zu definieren. Wenn Sie einen Job regelmäßig ausführen möchten und Sie nicht mithilfe der Web-Benutzeroberfläche planen können, können Sie ein Skript erstellen, um einen solchen Ablaufplan zu definieren. Sie möchten zum Beispiel immer am letzten Samstag im Monat eine Sicherung um 22:00 Uhr ausführen. Sie können einen solchen Ablaufplan nicht mithilfe der Web-Benutzeroberfläche definieren, aber Sie können hierfür ein entsprechendes Skript erstellen.

Sie können einen Sicherungsjob übergeben, ohne einen Ablaufplan anzugeben (mithilfe der Option Keine auf der Seite "Erweitert"). Verwenden Sie den Linux-Cron-Planer, um Ihren angepassten Ablaufplan zu definieren, und führen Sie den Befehl "*d2djob*" aus, um den Job auszuführen.

Hinweis: Bei dem folgenden Vorgang wird davon ausgegangen, dass Sie einen Sicherungsjob übergeben haben, ohne einen Ablaufplan anzugeben, und dass Sie am letzten Samstag jeden Monats eine Sicherung um 22:00 Uhr ausführen möchten.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Erstellen Sie eine Skriptdatei, und geben Sie den folgenden Befehl ein, um am letzten Samstag jeden Monats eine Sicherung um 22:00 Uhr auszuführen:

   ```
   #!/bin/bash

   LAST_SAT=$(cal | awk '$7!=""{t=$7} END {print t}')

   TODAY=$(date +%d)

   if [ "$LAST_SAT" = "$TODAY" ]; then

               source /opt/CA/d2dserver/bin/setenv

              d2djob --run=your_job_name   --jobtype=your_job_type      #run your
       backup job here

   fi
   ```

   Hinweis: Geben Sie der Datei die notwendigen Ausführungsberechtigungen.
3. Navigieren Sie zum Ordner "crontab", und fügen Sie den folgenden Befehl zum crontab des Systems hinzu (/etc/crontab):

   ```
   00 22 * * Saturday root runjob.sh
   ```

   Cron führt das Skript runjob.sh jeden Samstag um 22:00 Uhr aus. Mit runjob.sh wird zuerst geprüft, ob heute der letzte Samstag im Monat ist. Wenn dies der Fall ist, wird d2djob verwendet, um den Sicherungsjob auszuführen.

Der Jobablaufplan wurde so angepasst, dass am letzten Samstag jeden Monats eine Sicherung um 22:00 Uhr ausgeführt wird.

Ausführen eines BMR-Batch-Jobs

Wenn Sie eine BMR auf mehreren Rechnern ausführen möchten, und Sie die gleiche Betriebsumgebung auf allen Rechnern installieren möchten, dann können Sie eine Batch-BMR ausführen. Sie müssen keinen Job für jeden BMR-Job erstellen. Sie können Zeit und Aufwand sparen, und Sie können das Fehlerrisiko während der Konfiguration der BMR-Rechner reduzieren.

Hinweis: Sie müssen über einen gültigen Wiederherstellungspunkt des Quellrechners verfügen, den Sie wiederherstellen möchten. Wenn Sie keinen gültigen Wiederherstellungspunkt haben, müssen Sie zuerst den Quellrechner sichern und anschließend einen Wiederherstellungsjob übergeben.

Zunächst definieren Sie Ihre gesamten BMR-Einstellungen in einem Vorlagen-BMR-Job, und anschließend ändern Sie die Adresse des Zielcomputers (IP oder MAC), den Hostnamen und die Netzwerkkonfiguration, indem Sie folgenden Befehl verwenden:

```
d2djob
```

Gehen Sie wie folgt vor:

1. Erstellen Sie einen BMR-Job mit dem Namen "BMR-TEMPLATE", und führen Sie den Job für einen Rechner Ihrer mehreren Rechner aus.

   Hinweis: Sie können einen beliebigen Namen für den BMR-Job angeben. Sie müssen den gleichen Jobnamen im Batch-BMR-Skript angeben.

2. Melden Sie sich als root-Benutzer beim Sicherungsserver an.

3. Erstellen Sie ein Batch-BMR-Skript, das auf dem Job "BMR-TEMPLATE" basiert, um mehrere BMR-Jobs automatisch zu übergeben. Verwenden Sie folgendes Skript, um ein Batch-BMR-Skript zu erstellen:

   ```
   #!/bin/sh
   prename=lab-server
   serverList[0]="<MAC_Address>"
   serverList[1]=" <MAC_Address>"
   serverList[2]=" <MAC_Address>"
   .
   .
   .
   serverList[300]=" <MAC_Address>"
   for((i=0;i<${#serverList[@]};i=i+1))
   do
   ./d2djob --newrestore="BMR-TEMPLATE" --target=${serverList[i]}
   --hostname=$prename$i --network=dhcp
   done
   ```

4. Führen Sie das Batch-BMR-Skript aus.

   Das Skript wird ausgeführt. Mehrere BMR-Jobs werden in der Benutzeroberfläche erstellt.

Ein Batch-BMR-Job wird ausgeführt.

Replizieren und Verwalten von Sicherungssitzungen

Sie können ein Skript erstellen, um Ihre Sicherungssitzungen zu replizieren, sodass Sie Ihre Daten wiederherstellen können, wenn Ihre ursprünglichen Sicherungsdaten beschädigt sind. Die Sicherungssitzungen enthalten alle Wiederherstellungspunkte, die gesichert wurden. Sie können Ihre Sicherungssitzungen schützen, indem Sie Ihre Sicherungssitzungen in einem Replikationsziel replizieren.

Nachdem Sie Ihre Sicherungssitzungen repliziert haben, können Sie Ihr Replikationsziel verwalten, indem Sie der Arcserve UDP Agent (Linux)-Schnittstelle das Ziel hinzufügen.

Das Replizieren und Verwalten von Sicherungssitzungen ist ein dreiteiliger Prozess. Es besteht aus den folgenden drei Teilen:

- Replizieren der Sicherungssitzungen zum Replikationsziel
- Das Erstellen oder Aktualisieren der Konfigurationsdateien der Wiederherstellungspunkte, sodass Wiederherstellungspunkte verwaltet und auf der Arcserve UDP Agent (Linux)-Webschnittstelle angezeigt werden können
- Hinzufügen des Replikationsziels zur Arcserve UDP Agent (Linux)-Webschnittstelle

Replizieren der Sicherungssitzungen

Sie können die Funktion in Einstellungen für Prä-/Post-Skripts im Sicherungsassistenten nutzen, um die Sicherungssitzungen im Replikationsziel zu replizieren. Sie können eine beliebige Option, wie z. B. "File Transfer Protocol" (FTP), "Secure Copy" (SCP) oder den cp-Befehl auswählen, um die Sicherungssitzung zu replizieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Erstellen Sie ein Prä-/Post-Skript, um die Sicherungssitzungen zu replizieren.
3. Fügen Sie das Skript in folgenden Speicherort ein:

   `/opt/CA/d2dserver/usr/prepost`
4. Melden Sie sich bei der Arcserve UDP Agent (Linux)-Webbenutzeroberfläche an.
5. Öffnen Sie den Sicherungsassistenten, und navigieren Sie zur Seite Erweitert.
6. Wählen Sie in der Option "Einstellungen für Prä-/Post-Skripts" für "Auf Sicherungsserver ausführen" das Replikationsskript aus der Drop-down-Liste "Nach Abschluss des Jobs" aus.
7. Stellen Sie den Sicherungsjob in die Warteschlange.

Die Sicherungssitzung wird im Sicherungsziel repliziert.

Erstellen oder Aktualisieren der Konfigurationsdateien der Wiederherstellungspunkte

Nachdem Sie die Sicherungssitzungen repliziert haben, erstellen und konfigurieren Sie die Konfigurationsdatei der Wiederherstellungspunkte. Diese Datei wird verwendet, um die Wiederherstellungspunkte zu identifizieren, wenn Sie den Wiederherstellungsvorgang über die Arcserve UDP Agent (Linux)-Schnittstelle ausführen.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Navigieren Sie zu folgendem Speicherort:

   ```
   /opt/CA/d2dserver/bin
   ```

3. Geben Sie folgenden Befehl ein, um die Konfigurationsdatei der Wiederherstellungspunkte zu erstellen oder zu aktualisieren:

   ```
   ./d2drp --storagepath=/backupdestination --node=node_name
   --session=session_name
   ```

   Wenn Sie nur die Informationen *--storagepath* und *--node* angeben, dann aktualisiert der Befehl alle Sicherungssitzungen für den ausgewählten Knoten. Wenn Sie die Informationen *--session* angeben, dann aktualisiert der Befehl die spezifischen Sitzungsinformationen.

   Hinweis: Weitere Informationen über den Befehl "d2drp" finden Sie unter *Kennenlernen der Skripterstellungs-Hilfsprogramme*.

Die Konfigurationsdatei der Wiederherstellungspunkte wird erstellt oder je nach Status der Datei aktualisiert.

Hinzufügen des Replikationsziels

Fügen Sie der Arcserve UDP Agent (Linux)-Schnittstelle das Replikationsziel hinzu, um das Ziel zu verwalten. Nachdem Sie das Replikationsziel hinzugefügt haben, können Sie den verfügbaren freien Speicherplatz in diesem Ziel anzeigen und Ihre Daten entsprechend verwalten.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Replikationsziel an.
2. Erstellen Sie eine Datei mit dem Namen "Settings", und geben Sie folgenden Code in die Datei ein:

   ```
   RecoverySetLimit=n
   ```

   n stellt die Anzahl der Wiederherstellungssätze dar, die Sie im Replikationsziel beibehalten möchten.

3. Ordnen Sie die Datei im Knotenordner des Replikationsziels ein.

   Zum Beispiel "/backup_destination/node_name/Settings"

4. Melden Sie sich bei der Arcserve UDP Agent (Linux)-Webbenutzeroberfläche an.

5. Fügen Sie das Replikationsziel aus dem Menü Sicherungsspeicher hinzu.

Das Replikationsziel ist zur Arcserve UDP Agent (Linux)-Webschnittstelle hinzugefügt.

Die Sicherungssitzungen wurden erfolgreich repliziert und verwaltet.

Überprüfen, ob die Wiederherstellungspunkte verwendet werden können

Das d2dverify-Hilfsprogramm ist hilfreich bei der Überprüfung, ob die Wiederherstellungspunkte verschiedener Sicherungssitzungen brauchbar sind. Üblicherweise werden Sicherungsjobs täglich ausgeführt. Wenn Sie mehrere Wiederherstellungspunkte haben, sind Sie möglicherweise nicht sicher, ob diese Wiederherstellungspunkte für eine Datenwiederherstellung bei einem Systemausfall brauchbar sind. Um solche Situationen zu vermeiden, können Sie BMR-Jobs ausführen, um regelmäßig zu überprüfen, ob die Sicherungen brauchbar sind. Das d2dverify-Hilfsprogramm hilft Ihnen dabei, die Aufgabe zur Überprüfung der Brauchbarkeit von Wiederherstellungspunkten zu automatisieren.

Nachdem Sie die erforderlichen Parameter eingerichtet haben, übergibt das d2dverify-Hilfsprogramm den BMR-Job und stellt die Daten auf der angegebenen VM wieder her. Anschließend startet d2dverify die VM und führt ein Skript aus, um zu überprüfen, ob die Anwendungen auf der VM ordnungsgemäß funktionieren. Sie können auch mithilfe von Systemhilfsprogrammen wie Linux Cron einen Ablaufplan erstellen, um das d2dverify-Hilfsprogramm regelmäßig auszuführen. Zum Beispiel können Sie das d2dverify-Hilfsprogramm nach der letzten Sicherung eines Wiederherstellungssatzes ausführen. In diesem Fall überprüft d2dverify alle Wiederherstellungspunkte im spezifischen Wiederherstellungssatz.

Hinweis: Weitere Informationen zum Planen von Jobs unter Verwendung des Linux Cron-Planers finden Sie unter Anpassen des Job-Ablaufplans.

Das d2dverify-Hilfsprogramm kann auch in den folgenden Szenarien verwendet werden:

- Sie können das d2dverify-Hilfsprogramm verwenden, um die Sicherungen von mehreren physischen Rechnern zu virtuellen Rechnern zu migrieren.
- Nach der Wiederherstellung eines Hypervisor können Sie das d2dverify-Hilfsprogramm verwenden, um alle VMs am neuen Hypervisor wiederherzustellen.

Beachten Sie die folgenden Voraussetzungen, bevor Sie das d2dverify-Hilfsprogramm verwenden:

- Identifizieren Sie die Quellknoten, für die Sie die Sicherung überprüfen möchten.
- Identifizieren Sie einen Hypervisor, auf dem die VMs erstellt werden sollen.
- Erstellen Sie VMs für alle Knoten, die Sie überprüfen möchten. Weisen Sie den VM-Namen im folgenden Format zu:

  `verify_<Knotenname>`

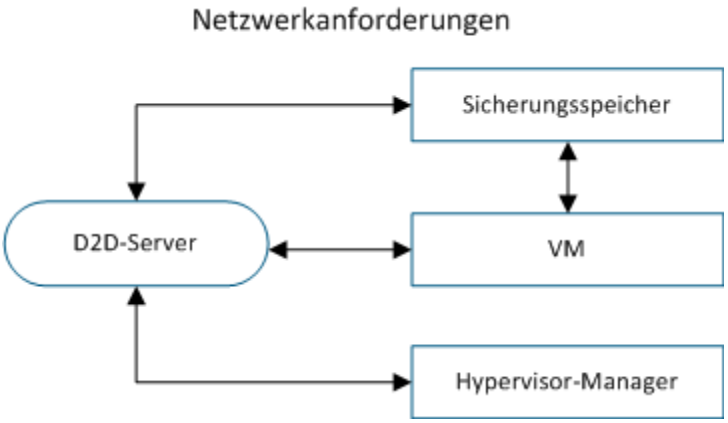
  Hinweis: Sie müssen für diese VMs keine virtuellen Festplatten anhängen. Darüber hinaus dürfen Sie an diese VMs kein virtuelles Netzwerk anhängen, wenn Sie vm_network-Parameter angegeben haben.
- Überprüfen Sie die Netzwerkanforderungen
- Identifizieren Sie ein Netzwerk für die Verbindung der VMs.

Hinweis: Das d2dverify-Hilfsprogramm unterstützt nur das statische IP-Netzwerk.

Wichtig! Wenn die Kontoinformationen der Datenbank mit einem Benutzer ohne root-Berechtigungen verknüpft sind, setzt d2dverify das Kennwort dieses Benutzers für die Ziel VM auf "CAd2d@2013" zurück.

Netzwerkanforderungen:

Wenn Sie d2dverify verwenden, wird empfohlen, für die Ziel-VMs ein isoliertes virtuelles Netzwerk zu verwenden, um Konflikte mit der Produktionsumgebung zu vermeiden. In solchen Fällen müssen die Ziel-VMs sowohl mit dem Sicherungsserver als auch mit dem Sicherungsspeicher verbunden sein.



Unterstützte Hypervisors:

Für die Durchführung der Wiederherstellung besteht eine d2dverify-Abhängigkeit vom d2drestorevm-Hilfsprogramm. d2dverify unterstützt die folgenden Hypervisor-Versionen:

- XenServer 6.0 und höher
- RHEV 3.0 und höher
- OVM 3.2

Parameter:

--template

Identifiziert die Vorlage, die die Parameter für die Ausführung des d2dverify-Hilfsprogramms enthält.

--createtemplate

Erstellt eine leere Vorlage, die die Parameter für die Ausführung des d2dverify-Hilfsprogramms enthält.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Erstellen Sie mithilfe des folgenden Befehls die Vorlage, die vom d2dverify-Hilfsprogramm verwendet wird:

   ```
   d2dverify --createtemplate=file_path
   ```

3. Öffnen Sie die Vorlage, und aktualisieren Sie die folgenden Parameter:

   node_list

   Gibt eine Liste von Knoten oder ein Kriterium für die Abfrage von Informationen aus der Datenbank des Sicherungsservers an. Die einzelnen Knoten werden durch Kommas abgetrennt (Node1,Node2,Node3).

   Hinweis: Wenn es sich bei der SSH-Portnummer nicht um Standardport 22 handelt, ist das Format für die Angabe der einzelnen Knoten "Node1:new_port,Node2:new_port,Node3:new_port". Der VM-Name wird im Format "verify_<Knotenname>" zugewiesen, wobei der die Portnummer nicht im Knotennamen enthalten ist.

   Beispiel: Node1:222,Node2:333,Node4:333

   Die folgende Liste ist ein Beispiel für Abfragekriterien:

   [node=prefix]

   Findet den Knotennamen, der das definierte Präfix enthält.

   [desc=prefix]

   Findet die Knotenbeschreibung, die das definierte Präfix enthält.

   guest_ip_list =

   Gibt die Liste von IP-Adressen an, die jeweils für die Zielknoten angewendet werden. Die einzelnen IP-Adressen werden durch Kommas voneinander getrennt (IP1,IP2,IP3). Wenn nur eine IP-Adresse verfügbar ist, aber mehrere Knoten im Parameter "node_list" vorhanden sind, wird das vierte Segment der IP-Adresse für jeden Knoten jeweils um 1 erhöht. Das d2dverify-Hilfsprogramm überprüft, ob diese IP-Adressen bereits verwendet wurden. In diesem Fall wird die entsprechende IP-Adresse übersprungen.

   Wenn Sie beispielsweise die drei Knoten "Knoten 1", "Knoten 2" und "Knoten 3" und eine IP-Adresse, "xxx.xxx.xxx.xx6", verwenden, wird die IP-Adresse wie in der folgenden Liste veranschaulicht verwendet:

   Knoten 1: xxx.xxx.xxx.xx6

   Knoten 2: xxx.xxx.xxx.xx7

   Knoten 3: xxx.xxx.xxx.xx8

vm_type

Gibt den Typ des Hypervisor an. Die folgenden drei Hypervisor-Typen sind gültig: xen, ovm und rhev.

vm_server

Gibt den Hostnamen oder die IP-Adresse des Hypervisor-Managers an.

vm_svr_username

Gibt den Benutzernamen des Hypervisor-Managers an.

vm_svr_password

Gibt das Kennwort des Hypervisor-Managers an. Das Kennwort muss mithilfe des Hilfsprogramms "d2dutil –encrypt" verschlüsselt werden.

Der folgende Befehl wird verwendet, um das Kennwort zu verschlüsseln:

```
echo "password" | d2dutil --encrypt
```

vm_network

Gibt das virtuelle Netzwerk an, das von der Ziel-VM verwendet wird. Es wird empfohlen, diesen Parameter anzugeben, wenn Ihre Ziel-VM mit mehreren virtuellen Netzwerken verbunden ist.

guest_gateway

Gibt das Netzwerk-Gateway an, das vom Gastbetriebssystem (BS) der Ziel-VM verwendet wird.

guest_netmask

Gibt die Netzmaske an, die vom Gastbetriebssystem der Ziel-VM verwendet wird.

guest_username

Gibt den Benutzernamen an, der für die Verbindung mit der wiederhergestellten VM verwendet wird. Das Kennwort wird auf das Kennwort zurückgesetzt, das im Parameter "guest_password" angegeben ist. Der Parameter "guest_username" wird ignoriert, wenn Sie das d2dverify-Hilfsprogramm verwenden, um Informationen aus der Datenbank des Sicherungsservers abzufragen. In diesem Fall wird das VM-Gastkennwort auf das Kennwort des Knotens zurückgesetzt, das in Datenbank gespeichert ist.

guest_password

Gibt das Kennwort für Parameter "den guest_username" an. Das Kennwort muss mithilfe des Hilfsprogramms "d2dutil –encrypt" verschlüsselt werden. Der Parameter "guest_password" wird ignoriert, wenn Sie das d2dverify-Hilfsprogramm verwenden, um Informationen aus der Datenbank des Sicherungsservers abzufragen.

storage_location

Gibt den Netzwerkpfad des Speicherorts der Sicherung an. Sie müssen den Speicherort nicht angeben, wenn sich die Knoten im Parameter "node_list" in der Datenbank des Sicherungsservers befinden. Wenn es sich beim Speicherort um eine CIFS-Freigabe handelt, geben Sie den Speicherort im folgenden Format an:

```
//Hostname/Pfad
```

storage_username

Gibt den Benutzernamen an, mit dem auf den Speicherort der Sicherung zugegriffen werden soll. Für NFS-Freigaben ist dieser Parameter nicht erforderlich.

Geben Sie den Speicherort für Benutzer von Windows-Domänen im folgenden Format an:

```
Domänenname/Benutzername
```

storage_password

Gibt das Kennwort an, mit dem auf den Speicherort der Sicherung zugegriffen werden soll. Das Kennwort muss mithilfe des Hilfsprogramms "d2dutil –encrypt" verschlüsselt werden. Für NFS-Freigaben ist dieser Parameter nicht erforderlich.

recovery_point = last

Gibt die Sitzung an, die Sie wiederherstellen möchten. Wiederherstellungssitzungen werden üblicherweise im Format "S00000000X" angegeben, wobei "X" für einen numerischen Wert steht. "S00000000X" ist der Ordnername der Wiederherstellungspunkte. Wenn Sie die letzte Sitzung wiederherstellen möchten, geben Sie das Schlüsselwort "last" an.

encryption_password

Gibt das Verschlüsselungskennwort für den Wiederherstellungspunkt an. Das Kennwort muss mithilfe des Hilfsprogramms "d2dutil –encrypt" verschlüsselt werden.

script

Gibt das Skript an, das Sie ausführen möchten. Das Skript wird nach einer erfolgreichen Wiederherstellung auf dem Zielcomputer ausgeführt. Wenn dieser Parameter nicht angegeben wird, führt das d2dverify-Hilfsprogramm den Befehl "ls /proc" auf dem Zielcomputer aus.

email_to_address

Gibt die E-Mail-Adresse der Empfänger an, die Berichte per E-Mail empfangen sollen. Sie können mehr als eine E-Mail-Adresse angeben. Trennen Sie sie durch Kommas voneinander ab.

email_subject

Gibt die Betreffzeile der E-Mail an.

report_format

Gibt das Format des Berichts an, den Sie per E-Mail empfangen werden. Das Format kann Text sein (.txt) oder html.

Standard: html

node_not_in_db

Gibt die Knoten der node_list-Parameter an, die sich nicht in der Datenbank des Sicherungsservers befinden. Sie müssen die Parameter angeben, die mit "storage_*" verknüpft sind.

Wert: yes

stop_vm_after_recovery

Gibt an, dass die Ziel-VM nach einer erfolgreichen Wiederherstellung und Prüfung angehalten werden soll. Die Werte für diesen Parameter sind "yes" und "no".

Standard: yes

4. Speichern und schließen Sie die Vorlage.
5. Führen Sie das d2dverify-Hilfsprogramm mithilfe des folgenden Befehls aus:

```
d2dverify --template=file_path
```

Hinweis: Das d2dverify-Hilfsprogramm schlägt fehl, wenn die Knoten im node_list-Parameter unter Verwendung des öffentlichen/privaten Schlüssels hinzugefügt werden. Um dieses Problem zu beheben, konfigurieren Sie die Umgebungsvariable "export D2D_SSH_IGNORE_PWD=yes" in der Shell-Umgebung, in der Sie das d2dverify-Hilfsprogramm ausführen.

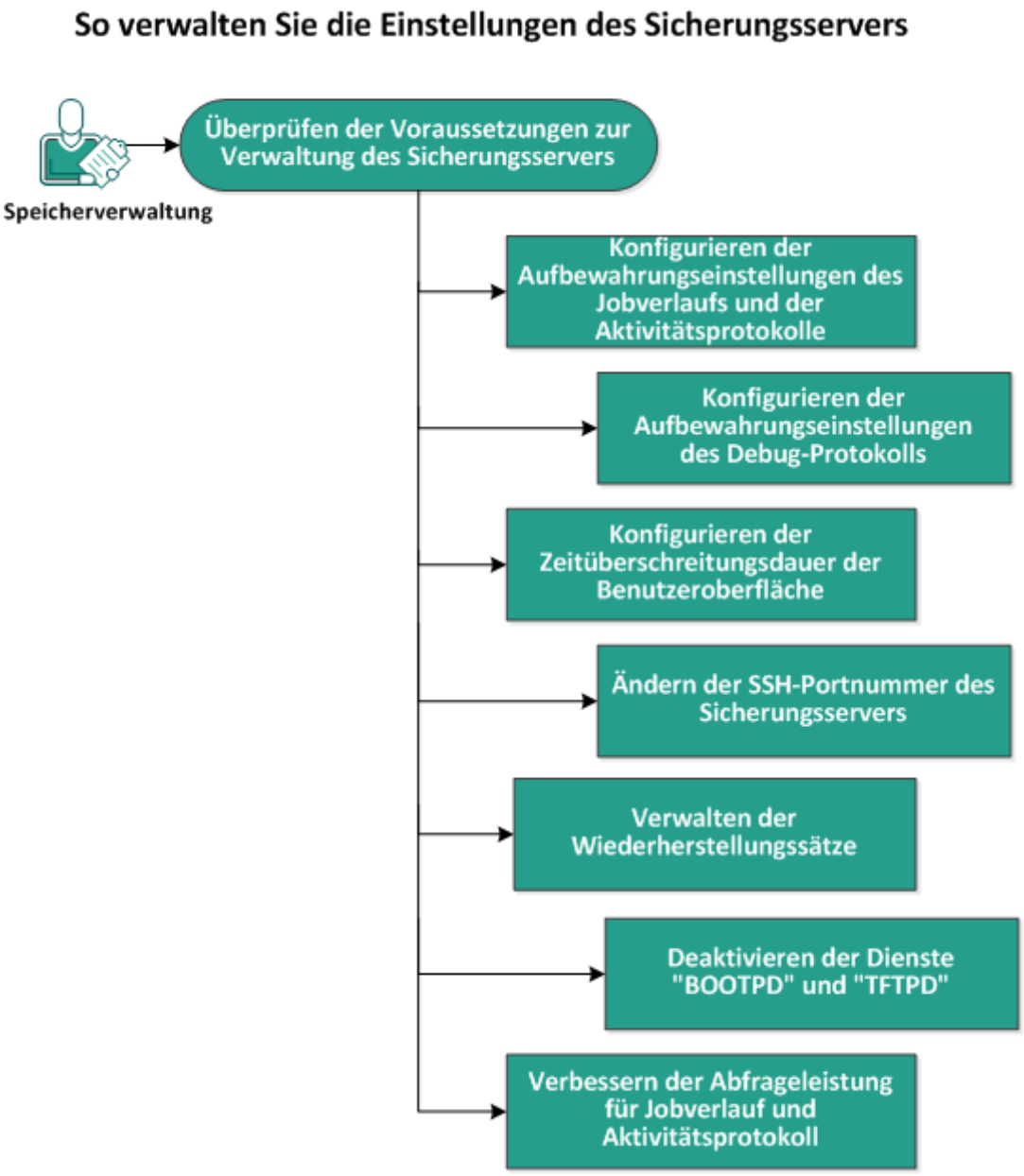
Die Brauchbarkeit von Wiederherstellungspunkten wurde erfolgreich überprüft.

So verwalten Sie die Einstellungen des Sicherungsservers

Sie können folgende Aufgaben ausführen, um den Sicherungsserver zu verwalten:

- Konfigurieren der Dauer, um den Jobverlauf und die Aktivitätsprotokolle beizubehalten
- Konfigurieren der Dauer, um die Debug-Protokolle beizubehalten
- Ändern der SSH-Portnummer (Secure Shell) des Sicherungsservers

Folgendes Diagramm zeigt den Vorgang an, um den Sicherungsserver zu verwalten:


So verwalten Sie die Einstellungen des Sicherungsservers
Speicherverwaltung
Überprüfen der Voraussetzungen zur Verwaltung des Sicherungsservers
Konfigurieren der Aufbewahrungseinstellungen des Jobverlaufs und der Aktivitätsprotokolle
Konfigurieren der Aufbewahrungseinstellungen des Debug-Protokolls
Konfigurieren der Zeitüberschreitungsdauer der Benutzeroberfläche
Ändern der SSH-Portnummer des Sicherungsservers
Verwalten der Wiederherstellungssätze
Deaktivieren der Dienste "BOOTPD" und "TFTPD"
Verbessern der Abfrageleistung für Jobverlauf und Aktivitätsprotokoll

Führen Sie folgende Aufgaben aus, um die Einstellungen des Sicherungsservers zu verwalten:

- Überprüfen der Voraussetzungen zur Verwaltung des Sicherungsservers (siehe Seite 179)
- Konfigurieren der Aufbewahrungseinstellungen des Jobverlaufs und der Aktivitätsprotokolle (siehe Seite 179)
- Konfigurieren der Aufbewahrungseinstellungen des Debug-Protokolls (siehe Seite 180)
- Konfigurieren der Zeitüberschreitungsdauer der Benutzeroberfläche (siehe Seite 181)
- Ändern der SSH-Portnummer des Sicherungsservers (siehe Seite 181)
- Verwalten der Wiederherstellungssätze (siehe Seite 182)
- Deaktivieren der Dienste "BOOTPD" und "TFTPD" (siehe Seite 183)
- Verbessern der Abfrageleistung für Jobverlauf und Aktivitätsprotokoll (siehe Seite 183)
- Überspringen der Prüfung von CIFS- und NFS-Clients (siehe Seite 184)

Überprüfen der Voraussetzungen zur Verwaltung des Sicherungsservers

Beachten Sie die folgenden Voraussetzungen, bevor Sie den Sicherungsserver verwalten:

- Sie verfügen über die root-Anmeldeinformationen für den Sicherungsserver.
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Konfigurieren der Aufbewahrungseinstellungen des Jobverlaufs und der Aktivitätsprotokolle

Sie können die Dauer konfigurieren, die der Jobverlauf und die Aktivitätsprotokolle beibehalten werden sollen. Wenn Sie die Aktivitätsprotokolle und den Jobverlauf für einen längeren Zeitraum beibehalten möchten, müssen Sie die Serverdatei konfigurieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Öffnen Sie die Datei "server.cfg":

   `/opt/CA/d2dserver/configfiles/server.cfg`

   Hinweis: Wenn die Datei nicht vorhanden ist, erstellen Sie die Datei "server.cfg".

3. Fügen Sie der Datei "server.cfg" folgende Zeile hinzu:

   ```
   job_history_activity_log_keep_day=<Anzahl von Tagen>
   ```

   Beispiel: Um den Jobverlauf und das Aktivitätsprotokoll für 30 Tage beizubehalten, geben Sie folgende Zeile ein:

   ```
   job_history_activity_log_keep_day=30
   ```

   Hinweis: Standardmäßig werden der Jobverlauf und die Aktivitätsprotokolle für 90 Tage beibehalten.

Der Jobverlauf und das Aktivitätsprotokoll werden für die angegebene Zeit beibehalten.

Konfigurieren der Aufbewahrungseinstellungen des Debug-Protokolls

Sie können die Dauer konfigurieren, die die Debug-Protokolle beibehalten werden sollen. Wenn Sie die Debug-Protokolle für einen längeren Zeitraum beibehalten möchten, müssen Sie die Serverdatei konfigurieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Öffnen Sie die Datei "server.cfg":

   ```
   /opt/CA/d2dserver/configfiles/server.cfg
   ```

   Hinweis: Wenn die Datei nicht vorhanden ist, erstellen Sie die Datei "server.cfg".
3. Fügen Sie der Datei "server.cfg" folgende Zeile hinzu:

   ```
   d2d_log_keep_day =<Anzahl von Tagen>
   ```

   Beispiel: Um das Debug-Protokoll für 30 Tage beizubehalten, geben Sie folgende Zeile ein:

   ```
   d2d_log_keep_day =30
   ```

   Hinweis: Standardmäßig werden Debug-Protokolle für 90 Tage beibehalten.

Das Arcserve UDP Agent (Linux)-Debug-Protokoll wird für den angegebenen Zeitraum beibehalten.

Konfigurieren der Zeitüberschreitungsdauer der Benutzeroberfläche

Sie können die Konfigurationsdatei des Webservers konfigurieren, sodass Sie aus der Benutzeroberfläche abgemeldet werden, wenn die Benutzeroberfläche inaktiv ist. Wenn Sie die Datei konfiguriert haben und innerhalb der angegebenen Dauer keine Aktivitäten in der Benutzeroberfläche stattfinden, dann werden Sie automatisch abgemeldet. Sie können sich erneut anmelden und Ihre Aktivitäten fortsetzen.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Öffnen Sie die Datei "server.cfg" von folgendem Speicherort:

   ```
   /opt/CA/d2dserver/configfiles/server.cfg
   ```

   Hinweis: Wenn die Datei "server.cfg" nicht vorhanden ist, dann erstellen Sie die Datei.
3. Fügen Sie der Datei "server.cfg" folgende Zeile hinzu:

   ```
   ui_timeout=<value>
   ```

   Der Wert muss in Minuten sein. Der Höchstwert für die Zeitüberschreitung der Benutzeroberfläche ist 60.

   Beispiel:

   ```
   ui_timeout=40
   ```

   Das Beispiel gibt an, dass der Benutzer abgemeldet wird, wenn der Sicherungsserver 40 Minuten lang keine Aktivität auf der Benutzeroberfläche feststellt.
4. Aktualisieren Sie den Webbrowser, um die Änderungen zu implementieren.

Die Dauer für die Zeitüberschreitung der Benutzeroberfläche ist konfiguriert.

Ändern der SSH-Portnummer des Sicherungsservers

Der Sicherungsserver verwendet für die Verbindung mit den Knoten den standardmäßigen SSH-Port 22. Wenn Sie den Standardport in einen anderen Port umändern möchten, können Sie den neuen Port über die Konfiguration der Datei "server.env" angeben.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.

2. Öffnen Sie die Datei "server.env".

   `/opt/CA/d2dserver/configfiles/server.env`

   Hinweis: Wenn die Datei nicht vorhanden ist, erstellen Sie die Datei "server.env".

3. Fügen Sie die folgende Zeile zur Datei "server.env" hinzu, und speichern Sie die Datei:

   `export D2D_SSH_PORT=new_port_number`

   "new_port_number" muss ein numerischer Wert sein.

4. Starten Sie den Sicherungsserver neu.

   Nachdem Sie die Datei "server.env" konfiguriert haben, verwenden alle Jobs mit Ausnahme des BMR-Jobs die neue Portnummer, um eine Verbindung mit dem Zielknoten herzustellen. Der BMR-Job verwendet den Standardport.

Die SSH-Portnummer des Sicherungsservers wurde erfolgreich geändert.

Verwalten der Wiederherstellungssätze

Das Verwalten der Wiederherstellungssätze umfasst das Löschen der Wiederherstellungssätze. Sie sollten Ihre Wiederherstellungssätze regelmäßig verwalten, um den verfügbaren freien Speicherplatz realistisch einschätzen zu können. Sie können die Speicherung der Wiederherstellungssätze dementsprechend planen. Es gibt zwei Methoden für die Verwaltung der Wiederherstellungssätze:

- **Methode 1:** Verwaltung mithilfe eines dedizierten Sicherungsspeichers. Mit dieser Methode werden die Wiederherstellungssätze alle 15 Minuten durch den Sicherungsspeicher verwaltet. Sie können nur jene Sicherungsspeicher verwalten, auf die der Sicherungsspeicher zugreifen kann. Wenn Sie als Sicherungsziel "Quelle - lokal" auswählen, müssen Sie den lokalen Ordner freigeben.
- **Methode 2:** Verwaltung mithilfe eines Sicherungsjobs. Mit dieser Methode werden die Wiederherstellungssätze durch den Sicherungsjob verwaltet. Die Wiederherstellungssätze werden nach Abschluss des Sicherungsjobs verwaltet. Sie können Wiederherstellungssätze verwalten, die in Ihrer lokalen Quelle gespeichert sind.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Öffnen Sie die Datei "server.cfg".

   `/opt/CA/d2dserver/configfiles/server.cfg`

   Hinweis: Wenn die Datei nicht vorhanden ist, erstellen Sie die Datei "server.cfg".

3. Fügen Sie die folgende Zeile zur Datei "server.cfg" hinzu, und speichern Sie die Datei:

   `manage_recoveryset_local=0 or 1`

Der Wert 0 zeigt an, dass die Datei Methode 1 verwendet.

Der Wert 1 zeigt an, dass die Datei Methode 2 verwendet.

4. Starten Sie den Sicherungsserver neu.

Die Wiederherstellungssätze werden über die Befehlszeile des Sicherungsspeichers verwaltet.

Deaktivieren der Dienste "BOOTPD" und "TFTPD"

Sie können die Dienste "BOOTPD" und "TFTPD" deaktivieren, wenn Sie die PXE BMR-Funktion nicht benötigen.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Öffnen Sie die Datei "server.env".

   ```
   /opt/CA/d2dserver/configfiles/server.env
   ```

3. Aktualisieren Sie den folgenden Parameter in der Datei "server.env", und speichern Sie die Datei:

   ```
   export D2D_DISABLE_PXE_SERVICE=yes
   ```

4. Starten Sie den Sicherungsserver neu

   ```
   /opt/CA/d2dserver/bin/d2dserver restart
   ```

Die Dienste "BOOTPD" und "TFTPD" wurden erfolgreich deaktiviert.

Verbessern der Abfrageleistung für Jobverlauf und Aktivitätsprotokoll

Wenn Sie eine umfangreiche Datenbankdatei verwenden, nimmt das Abfragen von Jobverlauf und Aktivitätsprotokoll viel Zeit in Anspruch. Sie können die Abfragezeit für Jobverlauf und Aktivitätsprotokoll mithilfe bestimmter Schalter verbessern, um innerhalb von kurzer Zeit eine Ausgabe zu erhalten.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Öffnen Sie die Datei "server.cfg":

   ```
   /opt/CA/d2dserver/configfiles/server.cfg
   ```

   Hinweis: Wenn die Datei nicht vorhanden ist, erstellen Sie die Datei "server.cfg".

3. Fügen Sie der Datei "server.cfg" die folgenden Zeilen hinzu:
   - Um die Abfrage des Jobverlaufs zu verbessern, fügen Sie die folgende Zeile hinzu:

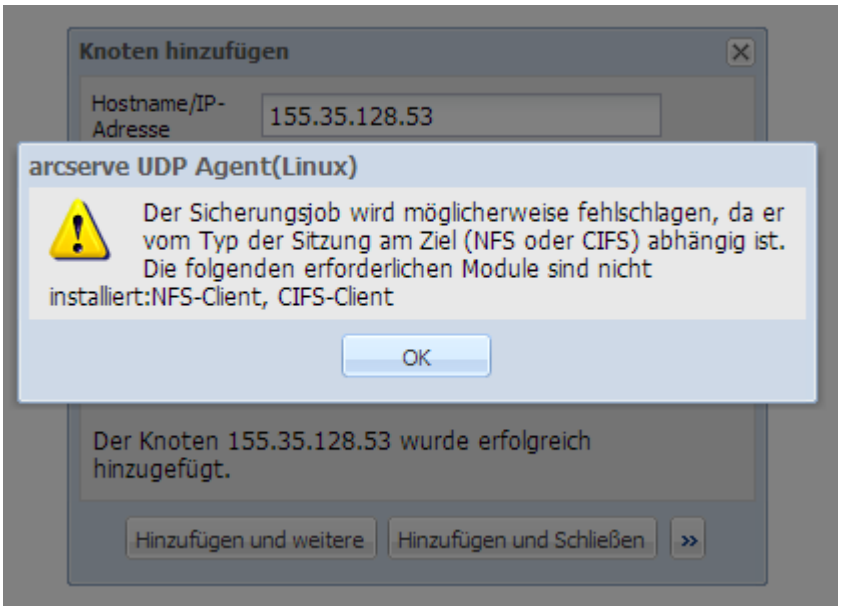
     ```
     skip_getting_job_history_count=true
     ```
   - Um die Abfrage des Aktivitätsprotokolls zu verbessern, fügen Sie die folgende Zeile hinzu:

     ```
     skip_getting_activity_log_count=true
     ```
4. Speichern Sie die Datei "server.cfg".

Die Abfragezeit für Jobverlauf und Aktivitätsprotokoll wurde erfolgreich verbessert.

Überspringen der Prüfung von CIFS- und NFS-Clients

Wenn Sie einen Knoten hinzufügen oder ändern, überprüft der Sicherungsserver die CIFS- und NFS-Module auf dem Zielknoten. Wenn eines dieser Module nicht installiert ist, wird ein Dialogfeld mit einer Warnung angezeigt. Sie können dieses Dialogfeld durch die Konfiguration der Datei server.cfg ausblenden.


Knoten hinzufügen
Hostname/IP-Adresse
155.35.128.53
arcserve UDP Agent(Linux)
Der Sicherungsjob wird möglicherweise fehlschlagen, da er vom Typ der Sitzung am Ziel (NFS oder CIFS) abhängig ist. Die folgenden erforderlichen Module sind nicht installiert:NFS-Client, CIFS-Client
OK
Der Knoten 155.35.128.53 wurde erfolgreich hinzugefügt.
Hinzufügen und weitere
Hinzufügen und Schließen
»

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Sicherungsserver an.
2. Öffnen Sie die Datei "server.cfg":

   `/opt/CA/d2dserver/configfiles/server.cfg`
3. Fügen Sie folgenden Parameter hinzu:

   `skip_client_check=client 1,client 2`

   Beispiel:

   `skip_client_check=nfs,cifs`

   Durch dieses Beispiel wird die Prüfung von NFS- und CIFS-Paketen auf dem Zielknoten übersprungen. Wenn Sie beide die Clients angeben, wird die Prüfung für beide Clients übersprungen. Wenn Sie nur einen Client angeben, wird die Prüfung nur für diesen Client übersprungen.
4. Speichern Sie die Datei "server.cfg".

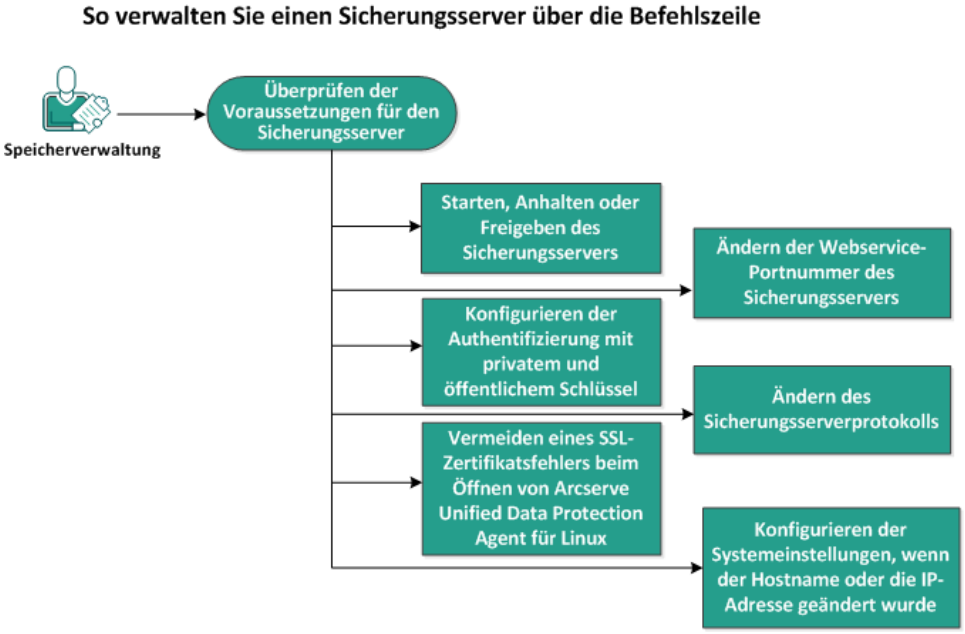
Die Prüfung wird für CIFS- und NFS-Clients übersprungen.

So verwalten Sie einen Linux-Sicherungsserver über die Befehlszeile

Der Linux-Sicherungsserver führt alle Verarbeitungsaufgaben von Arcserve UDP Agent (Linux) aus. Damit Arcserve UDP Agent (Linux) ordnungsgemäß ausgeführt werden kann, müssen Sie sicherstellen, dass der Sicherungsserver immer ausgeführt wird. Sie können sich beim Sicherungsserver anmelden und den Server mithilfe einiger Befehle verwalten.

Wenn Sie zum Beispiel auf die Web-Benutzeroberfläche von Arcserve UDP Agent (Linux) zugreifen möchten, müssen Sie sicherstellen, dass der Webserver läuft. Sie können den Ausführungsstatus des Webservers vom Sicherungsserver aus überprüfen und somit die ordnungsgemäße Funktion von Arcserve UDP Agent (Linux) sicherstellen.

Folgendes Diagramm zeigt den Vorgang an, um den Sicherungsserver über die Befehlszeile zu verwalten:


So verwalten Sie einen Sicherungsserver über die Befehlszeile
Speicherverwaltung
Überprüfen der Voraussetzungen für den Sicherungsserver
Starten, Anhalten oder Freigeben des Sicherungsservers
Ändern der Webservice-Portnummer des Sicherungsservers
Konfigurieren der Authentifizierung mit privatem und öffentlichem Schlüssel
Ändern des Sicherungsserverprotokolls
Vermeiden eines SSL-Zertifikatsfehlers beim Öffnen von Arcserve Unified Data Protection Agent für Linux
Konfigurieren der Systemeinstellungen, wenn der Hostname oder die IP-Adresse geändert wurde

Führen Sie folgende Aufgaben aus, um den Sicherungsserver zu verwalten:

- Überprüfen der Voraussetzungen für den Sicherungsserver (siehe Seite 186)
- Starten, Anhalten oder Freigeben des Sicherungsservers (siehe Seite 187)
- Ändern der Webservice-Portnummer des Sicherungsservers (siehe Seite 188)
- Konfigurieren der Authentifizierung mit privatem und öffentlichem Schlüssel (siehe Seite 189)
- Ändern des Sicherungsserverprotokolls (siehe Seite 190)
- Vermeiden des SSL-Zertifikatsfehlers beim Öffnen von Arcserve UDP Agent (Linux) (siehe Seite 191)
- Konfigurieren der Systemeinstellungen, wenn der Hostname oder die IP-Adresse geändert wurde (siehe Seite 193)

Überprüfen der Voraussetzungen für den Sicherungsserver

Beachten Sie die folgenden Voraussetzungen, bevor Sie den Sicherungsserver verwalten:

- Sie verfügen über die root-Anmeldeinformationen für den Sicherungsserver.
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Starten, Anhalten oder Freigeben des Sicherungsservers

Verwalten Sie den Sicherungsserver, um den Ausführungsstatus des Sicherungsservers zu kennen. Sie können überprüfen, ob der Sicherungsserver angehalten wurde oder noch läuft und den Server dann dementsprechend verwalten. Arcserve UDP Agent (Linux) unterstützt die folgenden Befehlszeilenfunktionen:

- Starten des Sicherungsservers
- Anhalten des Sicherungsservers
- Freigeben des Sicherungsservers

Gehen Sie wie folgt vor:

1. Navigieren Sie mit dem folgenden Befehl zum Ordner "bin":

   ```
   # cd/opt/CA/d2dserver/bin
   ```

   Sie haben Zugriff auf den Ordner "bin".

2. Führen Sie vom Ordner "bin" aus die folgenden Befehle aus (je nach der Aufgabe, die Sie für den Server durchführen möchten):

   Hinweis: Wenn keiner der Befehle erfolgreich ausgeführt werden kann, wird eine Fehlermeldung mit einer Erläuterung des Grundes angezeigt.

   ```
   # ./d2dserver start
   ```

   Startet den Sicherungsserver.

   Wenn dies erfolgreich ist, wird eine Meldung angezeigt, dass der Server gestartet wurde.

   ```
   # ./d2dserver stop
   ```

   Hält den Sicherungsserver an.

   Wenn dies erfolgreich ist, wird eine Meldung angezeigt, dass der Server angehalten wurde.

   ```
   # ./d2dserver restart
   ```

   Startet den Sicherungsserver neu.

   Wenn dies erfolgreich ist, wird eine Meldung angezeigt, dass der Server neu gestartet wurde.

```
# ./d2dserver status
```

Zeigt den Status des Sicherungsservers an.

```
# /opt/CA/d2dserver/bin/d2dreg --release
```

Gibt die verbleibenden Sicherungsserver frei, die vom Hauptserver verwaltet werden.

Zum Beispiel verwaltet Sicherungsserver-A zwei andere Server, Sicherungsserver-B und Sicherungsserver-C, wenn Sie dann Sicherungsserver-A deinstallieren, dann können Sie nicht auf Sicherungsserver-B und Sicherungsserver-C zugreifen. Sie können Sicherungsserver-B und Sicherungsserver-C mithilfe dieses Skripts freigeben, und Sie können auf diese Server zugreifen.

Der Sicherungsserver wurde erfolgreich von der Befehlszeile aus verwaltet.

Ändern der Webservice-Portnummer des Sicherungsservers

Arcserve UDP Agent (Linux) verwendet standardmäßig Port "8014". Wenn die Portnummer "8014" von einer anderen Anwendung verwendet wird, dann wird Arcserve UDP Agent (Linux) nicht ordnungsgemäß funktionieren. In solchen Fällen müssen Sie die Arcserve UDP Agent (Linux)-Standardportnummer in eine andere Portnummer ändern.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Datei "server.xml" von folgendem Speicherort:

   ```
   /opt/CA/d2dserver/TOMCAT/conf/server.xml
   ```

2. Suchen Sie folgende Zeichenfolge in der Datei, und ändern Sie die Portnummer "8014" in die gewünschte Portnummer:

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
   scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

3. Führen Sie folgenden Befehl aus, um den Sicherungsserver neu zu starten:

   ```
   /opt/CA/d2dserver/bin/d2dserver restart
   ```

Die Standardportnummer wird in Ihre gewünschte Portnummer geändert.

Konfigurieren der Authentifizierung mit privatem und öffentlichem Schlüssel

Mit dem öffentlichen Schlüssel und privaten Schlüssel können Sie eine sichere Verbindung mit dem Knoten herstellen, ohne das Kennwort anzugeben. Jedes Mal, wenn der Sicherungsserver eine SSH-Verbindung mit den Knoten erstellt, überprüft der Sicherungsserver den öffentlichen Schlüssel und den privaten Schlüssel für die jeweiligen Knoten. Wenn die Schlüssel nicht übereinstimmen, wird eine Fehlermeldung zurückgegeben.

Hinweis:

- Die Authentifizierung mit öffentlichem und privatem Schlüssel kann nur von Benutzern mit root-Berechtigungen verwendet werden. Der Benutzernamen muss dabei nicht "root" sein. Benutzer ohne root-Berechtigungen können die Authentifizierung mit öffentlichem und privatem Schlüssel nicht verwenden. Benutzer ohne root-Berechtigungen müssen sich mit Benutzernamen und Kennwort authentifizieren.
- Authentifizierung mit öffentlichem und privatem Schlüssel wird verwendet, wenn kein Kennwort angegeben wird. Der Benutzername ist weiterhin erforderlich und muss mit dem Eigentümer des Schlüssels übereinstimmen.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Generieren Sie mithilfe des folgenden ssh-keygen-Befehls einen öffentlichen/privaten Schlüssel:

   ```
   ssh-keygen -t rsa -f server
   ```

   Zwei Dateien werden generiert, nämlich server.pub und server.
3. Kopieren Sie die Datei des öffentlichen Schlüssels, "server.pub", an den folgenden Speicherort:

   ```
   /opt/CA/d2dserver/configfiles/server_pub.key
   ```
4. Kopieren Sie die Datei des privaten Schlüssels, "server", an den folgenden Speicherort:

   ```
   /opt/CA/d2dserver/configfiles/server_pri.key
   ```
5. (Optional) Führen Sie den folgenden Befehl aus, wenn Sie beim Generieren des privaten und öffentlichen Schlüssels die Passphrase angegeben haben:

   ```
   echo "passphrase" | d2dutil encrypt > /opt/CA/d2dserver/configfiles/key.pass
   ```
6. Ändern Sie mithilfe des folgenden Befehls die Berechtigungen für die Datei "key.pass":

   ```
   chmod 600 /opt/CA/d2dserver/configfiles/key.pass
   ```

7. Melden Sie sich beim Quellknoten an.
8. Kopieren Sie den Inhalt der Datei "server_pub.key" im Sicherungsserver an den folgenden Speicherort im Knoten:

   ```
   /root/.ssh/authorized_keys
   ```

Der private Schlüssel und der öffentliche Schlüssel wurden erfolgreich konfiguriert. Sie können mithilfe des öffentlichen und privaten Schlüssels eine Verbindung zum Quellknoten herstellen.

Ändern des Sicherungsserverprotokolls

Arcserve UDP Agent (Linux) ist mit dem https-Protokoll installiert. Sie können Ihr Protokoll ändern, wenn Sie Daten mit Verschlüsselung nicht übertragen möchten. Wir empfehlen Ihnen, https zu verwenden, da alle Daten, die mit https übertragen werden, verschlüsselt sind. Die mit http übertragenen Daten liegen als Klartext vor.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Datei "server.xml" von folgendem Speicherort:

   ```
   /opt/CA/d2dserver/TOMCAT/conf/server.xml
   ```

2. Suchen Sie folgende Zeichenfolge in der Datei "server.xml":

   ```
   <!--<Connector connectionTimeout="180000" port="8014" protocol="HTTP/1.1"/>-->
   ```

3. Entfernen Sie die Zeichen **<!--** und **-->**, wie im folgenden Beispiel dargestellt:

   Beispiel: Folgende Zeichenfolge ist die gewünschte Ausgabe, nachdem die Zeichen **<!--** und **-->** entfernt wurden:

   ```
   <Connector connectionTimeout="180000" port="8014" protocol="HTTP/1.1"/>
   ```

4. Suchen Sie folgende Zeichenfolge in der Datei "server.xml":

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
   scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

5. Fügen Sie die Zeichen **<!--** und **-->** hinzu, wie im folgenden Beispiel dargestellt:

   Beispiel: Folgende Zeichenfolge ist die gewünschte Ausgabe, nachdem die Zeichen **<!--** und **-->** hinzugefügt wurden:

   ```
   <!--<Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true"
   maxThreads="150" scheme="https" secure="true" clientAuth="false"
   sslProtocol="TLS" keystoreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>-->
   ```

6. Führen Sie folgenden Befehl aus, um den Sicherungsserver neu zu starten:

   ```
   /opt/CA/d2dserver/bin/d2dserver restart
   ```

Das Sicherungsserver-Protokoll wird von "https" in "http" geändert.

Vermeiden des SSL-Zertifikatsfehlers beim Öffnen von Arcserve UDP Agent (Linux)

Entfernen Sie das benutzerdefinierte SSL-Zertifikat, sodass Sie den Zertifikatsfehler nicht erhalten, wenn Sie die Arcserve UDP Agent (Linux)-Webbenutzeroberfläche öffnen. Sobald Sie das SSL-Zertifikat konfigurieren, werden Sie den Zertifikatsfehler nicht erneut erhalten.

Gehen Sie wie folgt vor:

- Verwenden Sie für den Firefox-Browser das von Arcserve UDP Agent (Linux) generierte Zertifikat.

  1. Öffnen Sie Arcserve UDP Agent (Linux) in Firefox.
  2. Klicken Sie auf "I Understand the Risks", und klicken Sie dann auf "Add Exception".

     Das Dialogfeld "Add Security Exception" wird geöffnet.
  3. Klicken Sie auf "View" , um das Zertifikat zu überprüfen.

     Das Dialogfeld "Certificate Viewer" wird geöffnet.
  4. Überprüfen Sie die Zertifikatsdetails, und klicken Sie auf "Schließen".

     Sie müssen im Dialogfeld "Certificate Viewer" keine Aktion ausführen.
  5. Wählen Sie im Dialogfeld "Add Security Exception" das Kontrollkästchen "Permanently store this exception" aus.
  6. Klicken Sie auf "Confirm Security Exception".

     Das Zertifikat wird hinzugefügt.

- Verwenden Sie das von Arcserve UDP Agent (Linux) generierte Zertifikat für Internet Explorer (IE) oder Chrome.
  1. Öffnen Sie Arcserve UDP Agent (Linux) in IE oder in Chrome.
  2. Klicken Sie auf "Laden dieser Website fortsetzen (nicht empfohlen)".

     Der Adressbalken wird rot angezeigt, und eine Zertifikatsfehlermeldung wird in der Sicherheitsstatusleiste angezeigt.
  3. Klicken Sie auf "Zertifikatfehler".

     Das Dialogfeld "Nicht vertrauenswürdiges Zertifikat" wird angezeigt.
  4. Klicken Sie auf "Zertifikate anzeigen".

     Das Dialogfeld "Certificate" wird geöffnet.
  5. Klicken Sie auf der Registerkarte "Allgemein" auf "Zertifikat installieren".

     Der Zertifikatimport-Assistent wird angezeigt.
  6. Klicken Sie auf "Weiter".
  7. Wählen Sie auf der Seite "Zertifikatsspeicher" die Option "Alle Zertifikate in folgendem Speicher speichern" aus, und klicken Sie dann auf "Durchsuchen".

     Das Dialogfeld "Select Certificate Store" wird angezeigt:
  8. Wählen Sie "Vertrauenswürdige Stammzertifizierungsstellen" aus, und klicken Sie auf "OK".

     Die Seite "Zertifikatsspeicher" des Zertifikatimport-Assistenten wird geöffnet.
  9. Klicken Sie auf "Weiter" und anschließend auf "Fertig stellen".

     Das Dialogfeld "Sicherheitswarnung" wird angezeigt.
  10. Klicken Sie auf "Ja".
  11. Starten Sie IE oder Chrome neu.

      Das Zertifikat wird hinzugefügt.

      Hinweis: Nachdem Sie das Zertifikat hinzugefügt haben, zeigt der Chrome-Browser weiterhin das Fehlersymbol für das SSL-Zertifikat in der Adressleiste an. Dies ist eine Erinnerung daran, dass das Zertifikat nicht von allen Zertifikatstellen identifiziert wird, jedoch erkennt Chrome dieses Zertifikat, und alle ins Netzwerk übertragene Daten sind verschlüsselt.
- Führen Sie folgende Schritte aus, um ein signiertes Zertifikat zu verwenden:
  1. Verwenden Sie das Zertifikat, das von einer Zertifizierungsstelle signiert wurde.
  2. Importieren Sie das signierte Zertifikat mithilfe des Befehls "keytool".

     Das Zertifikat wird hinzugefügt.

Der SSL-Zertifikatsfehler ist gelöst.

Konfigurieren der Systemeinstellungen, wenn der Hostname oder die IP-Adresse geändert wurde

Wenn Sie den Hostnamen oder die IP-Adresse des Sicherungsservers oder den Client-Knoten (Sicherungsknoten) ändern, dann müssen Sie die Systemeinstellungen konfigurieren. Sie konfigurieren die Systemeinstellungen, um folgende Elemente sicherzustellen:

- Um sicherzustellen, dass die Kommunikation zwischen dem zentralen Server und dem Mitgliedsserver gut ist. Ein Mitgliedsserver ist ein Sicherungsserver, den Sie über den zentralen Sicherungsserver verwalten. Um den Mitgliedsserver über die Benutzeroberfläche des zentralen Servers zu verwalten, müssen Sie den Mitgliedsserver zur Benutzeroberfläche des zentralen Servers hinzufügen.
- Um sicherzustellen, dass Sie, nachdem Sie den Hostnamen oder die IP-Adresse des Client-Knotens geändert haben, den Client-Knoten fehlerfrei sichern können

Wenn der Hostname des zentralen Sicherungsservers geändert wird

Wenn Sie den Hostnamen des zentralen Sicherungsservers ändern, müssen Sie den Server konfigurieren, sodass Sie Arcserve UDP Agent (Linux) ohne Probleme verwenden können.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim zentralen Sicherungsserver an.
2. Um den Hostnamen und die Lizenzinformationen zu aktualisieren, geben Sie folgende Befehle ein:

   ```
   source /opt/CA/d2dserver/bin/setenv
   ```

   ```
   /opt/CA/d2dserver/sbin/sqlite3 /opt/CA/d2dserver/data/ARCserveLinuxD2D.db
   "update D2DServer set Name='New_Hostname' where IsLocal=1"
   ```

   ```
   /opt/CA/d2dserver/sbin/sqlite3 /opt/CA/d2dserver/data/License.db "update
   LicensedMachine set ServerName ='New_Hostname' where ServerName ='Old_Hostname'"
   ```

3. Benennen Sie die Schlüsselspeicherdatei um:

   ```
   mv /opt/CA/d2dserver/TOMCAT/conf/server.keystore
   /opt/CA/d2dserver/TOMCAT/conf/server.keystore.old
   ```

4. Erstellen Sie eine Schlüsselspeicherdatei, indem Sie den folgenden Java-Befehl "keytool" verwenden.

   ```
   keytool -genkey -alias tomcat -keyalg DSA -keypass <YOUR_VALUE> -storepass
   <YOUR_VALUE> -keystore /opt/CA/d2dserver/TOMCAT/conf/server.keystore -validity
   3600 -dname "CN=<New Hostname>"
   ```

   Hinweis: Aktualisieren Sie das Feld "YOUR_VALUE" entsprechend Ihrer Anforderung. Normalerweise ist der Wert Ihr Kennwort.

   Beispiel:

   ```
   keytool -genkey -alias tomcat -keyalg DSA -keypass LinuxD2D -storepass LinuxD2D
   -keystore /opt/CA/d2dserver/TOMCAT/conf/server.keystore -validity 3600 -dname
   "CN=New Hostname"
   ```

5. Öffnen Sie die TOMCAT-Konfigurationsdatei, und ändern Sie die Werte für keystoreFile und keystorePass entsprechend der Schlüsselspeicherdatei, die Sie soeben erstellt haben:

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
   scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="${catalina.home}/conf/server.keystore"
   keystorePass="YOUR_VALUE"/>
   ```

   Beispiel:

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
   scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

6. Starten Sie den zentralen Sicherungsserver neu.

   ```
   /opt/CA/d2dserver/bin/d2dserver restart
   ```

Der zentrale Sicherungsserver ist konfiguriert.

Wenn der Hostname oder die IP-Adresse des Mitgliedsservers geändert wurde

Wenn Sie den Hostnamen oder die IP-Adresse des Mitglieds-Sicherungsservers ändern, konfigurieren Sie den Mitgliedsserver, um ihn über den zentralen Server zu verwalten. Wenn Sie den Mitgliedsserver nicht konfigurieren, dann erhalten Sie einen Fehler, wenn Sie versuchen, den Mitgliedsserver über den zentralen Server zu verwalten. Ein Mitgliedsserver ist ein Server, den Sie der Webschnittstelle des zentralen Sicherungsservers hinzugefügt haben.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Mitglieds-Sicherungsserver an:
2. Um den Hostnamen zu ändern, geben Sie folgende Befehle ein:

   ```
   source /opt/CA/d2dserver/bin/setenv
   ```

   ```
   /opt/CA/d2dserver/sbin/sqlite3 /opt/CA/d2dserver/data/ARCserveLinuxD2D.db
   "update D2DServer set Name='New_Hostname' where IsLocal=1"
   ```

3. Benennen Sie die Schlüsselspeicherdatei um:

   ```
   mv /opt/CA/d2dserver/TOMCAT/conf/server.keystore
   /opt/CA/d2dserver/TOMCAT/conf/server.keystore.old
   ```

4. Erstellen Sie eine Schlüsselspeicherdatei, indem Sie den folgenden Java-Befehl "keytool" verwenden.

   ```
   keytool -genkey -alias tomcat -keyalg DSA -keypass <YOUR_VALUE> -storepass
   <YOUR_VALUE> -keystore /opt/CA/d2dserver/TOMCAT/conf/server.keystore -validity
   3600 -dname "CN=<New Hostname>"
   ```

   Hinweis: Aktualisieren Sie das Feld "YOUR_VALUE" entsprechend Ihrer Anforderung. Normalerweise ist der Wert Ihr Kennwort.

   Beispiel:

   ```
   keytool -genkey -alias tomcat -keyalg DSA -keypass LinuxD2D -storepass LinuxD2D
   -keystore /opt/CA/d2dserver/TOMCAT/conf/server.keystore -validity 3600 -dname
   "CN=New Hostname"
   ```

5. Öffnen Sie die TOMCAT-Konfigurationsdatei "server.xml", und ändern Sie den Wert keystoreFile und keystorePass entsprechend der Schlüsselspeicherdatei.

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
   scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="${catalina.home}/conf/server.keystore"
   keystorePass="YOUR_VALUE"/>
   ```

   Beispiel:

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
   scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

6. Starten Sie den Mitglieds-Sicherungsserver neu.

   ```
   /opt/CA/d2dserver/bin/d2dserver restart
   ```

7. Melden Sie sich bei der zentralen Arcserve Unified Data Protection Agent for Linux-Webschnittstelle an.
8. Wählen Sie im Bereich "Sicherungsserver" den alten Hostnamenserver aus.
9. Klicken Sie im Menü "Sicherungsserver" auf "Löschen".
10. Klicken Sie im Dialogfeld "Löschen" auf "OK".

    Der alte Hostnamenserver wird gelöscht.

11. Klicken Sie im Menü "Sicherungsserver" auf "Hinzufügen".

    Das Dialogfeld "Server hinzufügen" wird geöffnet.

12. Geben Sie die neuen Hostnamendetails in das Dialogfeld ein, und klicken Sie auf "OK".

    Das Dialogfeld "Server hinzufügen" wird geschlossen, und der Mitgliedsserver mit dem neuen Hostnamen wird der Benutzeroberfläche hinzugefügt.

13. Melden Sie sich beim zentralen Sicherungsserver an, der den Mitglieds-Sicherungsserver verwaltet.
14. Um die Lizenzinformationen zu aktualisieren, geben Sie die folgenden Befehle ein:

    ```
    source /opt/CA/d2dserver/bin/setenv
    ```

    ```
    /opt/CA/d2dserver/sbin/sqlite3 /opt/CA/d2dserver/data/License.db "update
    LicensedMachine set ServerName ='New_Hostname' where ServerName ='Old_Hostname'"
    ```

Der Mitglieds-Sicherungsserver ist konfiguriert.

Wenn der Hostname oder die IP-Adresse des Client-Knotens geändert wurde

Wenn Sie den Hostnamen oder die IP-Adresse eines Knotens ändern, können Sie den Hostnamen oder die IP-Adresse in den Systemeinstellungen konfigurieren, sodass Sie diesen Knoten fehlerfrei sichern können.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Sicherungsziel an.
2. Suchen Sie den Ordner "**Old_Hostname"** im Sicherungsziel dieses Knotens, und benennen Sie ihn in "**New_Hostname"** um.

   Beachten Sie zum Beispiel, dass "First_Node" der alte Hostnamen für "node1" ist. Das Sicherungsziel für "node1" ist "//Backup_Destination/LinuxBackup". Nach der ersten erfolgreichen Sicherung wird ein Ordner mit dem Namen "First_Node" in "//Backup_Destination/LinuxBackup" erstellt. Jetzt haben Sie den alten Hostnamen in "Second_Node" geändert. Suchen Sie den Ordner "First_Node" in "//Backup_Destination/LinuxBackup", und benennen den Ordner in "Second_Node" um.
3. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
4. Um den Hostnamen zu aktualisieren, geben Sie folgende Befehle ein:

   ```
   source /opt/CA/d2dserver/bin/setenv
   ```

   ```
   /opt/CA/d2dserver/bin/d2drp --storagepath=Backup Destination
   --node=New_Hostname
   ```

   ```
   /opt/CA/d2dserver/sbin/sqlite3 /opt/CA/d2dserver/data/ARCserveLinuxD2D.db
   "update JobQueue set TargetName='New_Hostname' where JobType in (1,3,4,5) and
   TargetName='Old_Hostname'"
   ```

   ```
   /opt/CA/d2dserver/sbin/sqlite3 /opt/CA/d2dserver/data/ARCserveLinuxD2D.db
   "update TargetMachine set Name='New_Hostname' where Name='Old_Hostname'"
   ```

   Hinweis: Wenn Sie "NFS-Freigabe" oder "CIFS-Freigabe" als Sicherungsziel verwenden, sollten Sie es als lokale Freigabe laden.

   Beispiel: Wenn Ihr Bereitstellungspunkt "/mnt/backup_destination" ist.

   ```
   /opt/CA/d2dserver/bin/d2drp --storagepath=<mount point>
   --node=New_Hostname
   ```

   Hinweis: Wenn Sie eine lokale Freigabe verwenden, dann ist der Befehl:

   ```
   /opt/CA/d2dserver/bin/d2drp --storagepath=<local path> --node=New_Hostname
   ```

5. Melden Sie sich als root-Benutzer beim zentralen Sicherungsserver an.
6. Um die Lizenzinformationen zu aktualisieren, geben Sie folgenden Befehl ein:

   ```
   /opt/CA/d2dserver/sbin/sqlite3 /opt/CA/d2dserver/data/License.db "update
   LicensedMachine set MachineName ='New_Hostname' where MachineName
   ='Old_Hostname'"
   ```

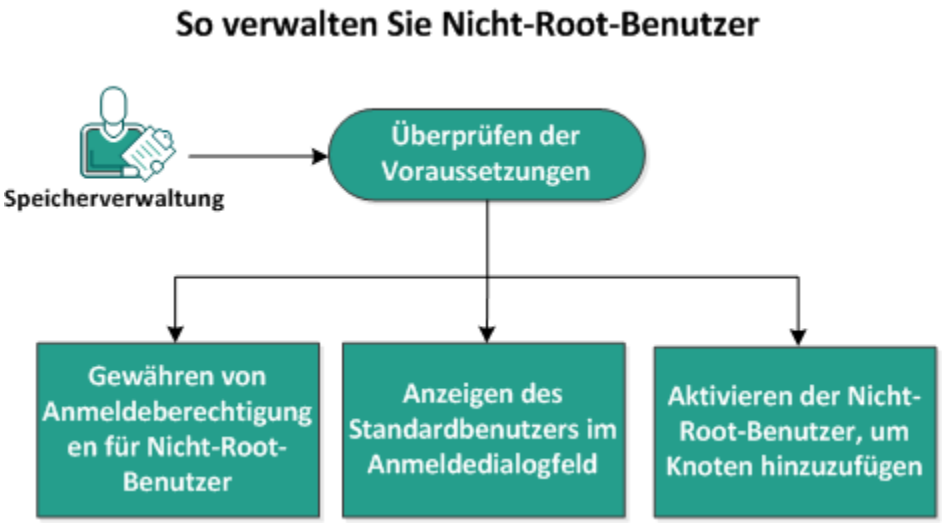
Der Hostname wird konfiguriert, um eine fehlerfreie Sicherung auszuführen.

So verwalten Sie Nicht-Root-Benutzer

Sie können Ihre gesamten Nicht-Root-Benutzer verwalten, die auf Arcserve UDP Agent (Linux) zugreifen, und Sie können die Berechtigungen für die Nicht-Root-Benutzer definieren, um die Zugriffsebene für Arcserve UDP Agent (Linux) zu beschränken. Sie können die Nicht-Root-Benutzer verwalten, indem Sie die Konfigurationsdatei des Webservers (Datei "server.cfg") ändern.

Hinweis: Wenn Ihr Sicherungsquellenknoten mit "pam_wheel" konfiguriert ist, dann verwenden Sie die Option "use_uid", um "pam_wheel" zu konfigurieren. Weitere Informationen zu "pam_wheel" finden Sie auf der man-Seite von pam_wheel.

Folgendes Diagramm zeigt den Vorgang zur Verwaltung von Nicht-Root-Benutzern:


So verwalten Sie Nicht-Root-Benutzer
Speicherverwaltung
Überprüfen der Voraussetzungen
Gewähren von Anmeldeberechtigungen für Nicht-Root-Benutzer
Anzeigen des Standardbenutzers im Anmeldedialogfeld
Aktivieren der Nicht-Root-Benutzer, um Knoten hinzuzufügen

Führen Sie diese Aufgaben aus, um die Nicht-Root-Benutzer zu verwalten:

- Überprüfen der Voraussetzungen (siehe Seite 199)
- Gewähren von Anmeldeberechtigungen für Nicht-Root-Benutzer (siehe Seite 199)
- Anzeigen des Standardbenutzers im Anmeldedialogfeld (siehe Seite 200)
- Aktivieren der Nicht-Root-Benutzer, um Knoten hinzuzufügen (siehe Seite 201)

Überprüfen der Voraussetzungen

Beachten Sie die folgenden Voraussetzungen, bevor Sie den Nicht-Root-Benutzer verwalten:

- Sie verfügen über die root-Anmeldeinformationen für den Sicherungsserver.
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Gewähren von Anmeldeberechtigungen für Nicht-Root-Benutzer

Ein Root-Benutzer kann Nicht-Root-Benutzern Berechtigungen zur Anmeldung auf dem Sicherungsserver gewähren. Wenn Nicht-Root-Benutzer die Berechtigung zur Anmeldung auf dem Sicherungsserver erhalten, können Sie Arcserve UDP Agent (Linux) verwenden, um alle Datenschutz- und Wiederherstellungsaufgaben durchzuführen.

Hinweis: Um den Nicht-Root-Benutzern Anmeldeberechtigungen zu gewähren, stellen Sie mithilfe der SSH-Verbindung eine Verbindung zum Sicherungsserver als Root-Benutzer her.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Öffnen Sie die Datei "server.cfg" von folgendem Speicherort:

   ```
   /opt/CA/d2dserver/configfiles/server.cfg
   ```

   Hinweis: Wenn die Datei "server.cfg" nicht vorhanden ist, dann erstellen Sie die Datei.
3. Fügen Sie der Datei "server.cfg" folgenden Code hinzu:

   ```
   allow_login_users=user1 user2
   ```

   Hinweis: Verwenden Sie Leerzeichen, um verschiedene Benutzer zu unterscheiden.

   Der Code wird hinzugefügt.
4. Stellen Sie sicher, dass der Nicht-Root-Benutzer mithilfe der SSH-Verbindung eine Verbindung zum Sicherungsserver herstellen kann.

Die Anmeldeberechtigung wird den Nicht-Benutzern gewährt, um auf den Sicherungsserver zuzugreifen.

Anzeigen des Standardbenutzers im Anmeldedialogfeld

Sie können Ihre Benutzer verwalten, und Sie können den Namen ändern, der im Anmeldedialogfeld von Arcserve UDP Agent (Linux) angezeigt wird. Der Standardbenutzer, der im Anmeldedialogfeld angezeigt wird, ist "Root". Wenn keine Root-Benutzer auf das Produkt zugreifen, dann können Sie den Standardnamen in einen beliebigen Nicht-Root-Benutzernamen ändern. Sie erreichen dies, indem Sie die Datei "server.cfg" ändern, die sich auf dem Sicherungsserver befindet.

Hinweis: Um die Datei "server.cfg" zu ändern, stellen Sie mithilfe der SSH-Verbindung eine Verbindung mit dem Sicherungsserver als Root-Benutzer her.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Öffnen Sie die Datei "server.cfg" von folgendem Speicherort:

   `/opt/CA/d2dserver/configfiles/server.cfg`

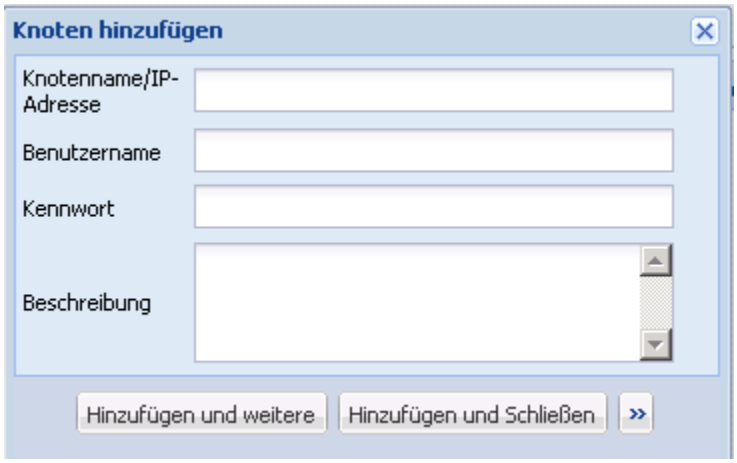
   Hinweis: Wenn die Datei "server.cfg" nicht vorhanden ist, dann erstellen Sie die Datei.
3. Fügen Sie der Datei "server.cfg" folgenden Code hinzu:
   show_default_user_when_login=false|true
4. Melden Sie sich bei der Arcserve UDP Agent (Linux)-Webbenutzeroberfläche an.
   - Wenn Sie den Befehl *allow_login_users* hinzugefügt haben, zeigt das Anmeldedialogfeld den ersten Benutzer an, der im Befehl *allow_login_users* hinzugefügt wurde.
   - Wenn Sie den Befehl *allow_login_users* nicht hinzugefügt haben, dann zeigt das Anmeldedialogfeld den Root-Benutzer an.

Der Standardbenutzer wird im Anmeldedialogfeld von Arcserve UDP Agent (Linux) angezeigt.

Aktivieren der Nicht-Root-Benutzer, um Knoten hinzuzufügen

Wenn der SSH-Server die Root-Benutzeranmeldung deaktiviert, können Sie die Anmeldung des Nicht-Root-Benutzers aktivieren, um Knoten hinzuzufügen. Wenn Sie die Anmeldeinformationen des Nicht-Root-Benutzers aktivieren, dann wird das Dialogfeld "Knoten hinzufügen" geändert, und die Option "Stammanmeldeinformationen" wird angezeigt.

Hinweis: Wenn Sie die Anmeldeinformationen des Client-Knotens von einem Root-Benutzer in einen Nicht-Root-Benutzer ändern, dann ist es empfehlenswert, den Ordner */tmp* auf dem Client-Knoten zu löschen, bevor Sie den Sicherungsjob ausführen.



Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Öffnen Sie die Datei "server.cfg" von folgendem Speicherort:

   `/opt/CA/d2dserver/configfiles/server.cfg`

   Hinweis: Wenn die Datei "server.cfg" nicht vorhanden ist, dann erstellen Sie die Datei.
3. Fügen Sie folgende Zeile in der Datei "server.cfg" hinzu, um die Funktion des Nicht-Root-Benutzers zu aktivieren:

   `enable_non_root_user=true`

   Die Funktion des Nicht-Root-Benutzers ist aktiviert.

4. (Optional) Fügen Sie folgende Zeile in der Datei "server.cfg" hinzu, um die Funktion des Nicht-Root-Benutzers zu deaktivieren:

   ```
   enable_non_root_user=false
   ```

   Die Funktion des Nicht-Root-Benutzers ist deaktiviert.

Die Nicht-Root-Benutzer können Knoten hinzufügen.

Hinweis: Wenn Sie das Kennwort für den Root-Benutzer oder für den Nicht-Root-Benutzer ändern und Sie anschließend den Knoten ändern, dann müssen Sie sowohl das Root-Kennwort als auch das Nicht-Root-Kennwort in ihren jeweiligen Feldern im Dialogfeld Knoten ändern erneut eingeben.

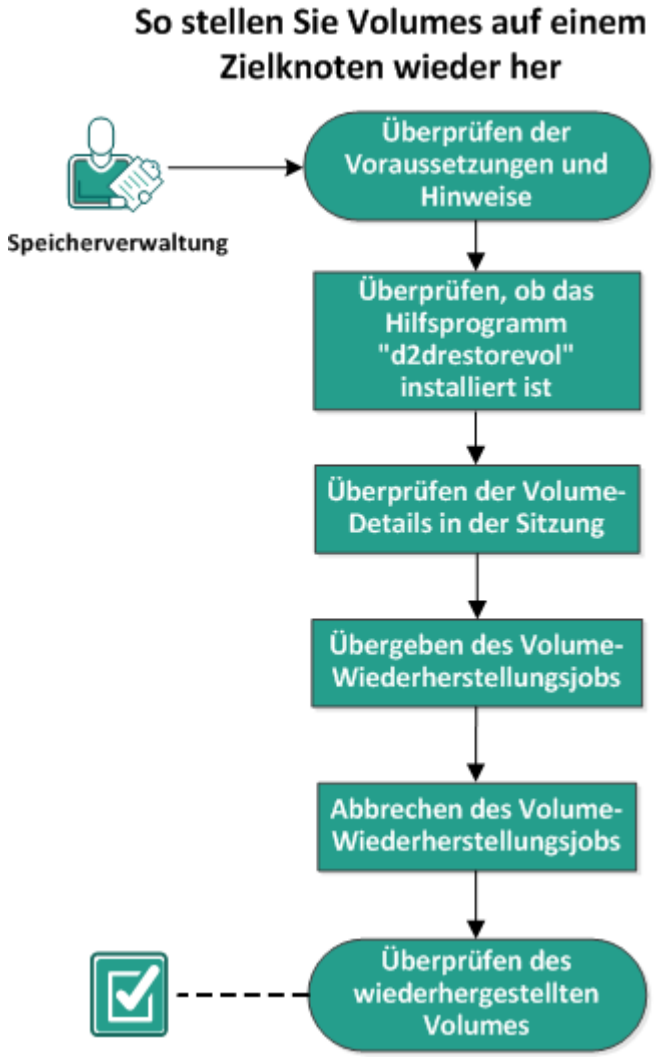
Hinweis: Die Nicht-Root-Benutzer können keine Knoten mithilfe des Befehls *d2dnode* über die Befehlszeile verwalten.

So stellen Sie Volumes auf einem Zielknoten wieder her

Sie können individuelle Volumes auf dem Zielknoten wiederherstellen, ohne dabei eine vollständige BMR auszuführen. Der Zielknoten kann ein Sicherungsserver oder ein geschützter Knoten sein.

Das Wiederherstellen von individuellen Volumes nutzt weniger Ressourcen und stellt eine bessere Leistung bereit.

Folgendes Diagramm zeigt den Vorgang zur Wiederherstellung von Volumes:


So stellen Sie Volumes auf einem Zielknoten wieder her
Speicherverwaltung
Überprüfen der Voraussetzungen und Hinweise
Überprüfen, ob das Hilfsprogramm "d2drestorevol" installiert ist
Überprüfen der Volume-Details in der Sitzung
Übergeben des Volume-Wiederherstellungsjobs
Abbrechen des Volume-Wiederherstellungsjobs
Überprüfen des wiederhergestellten Volumes

Führen Sie folgende Schritte durch, um Volumes wiederherzustellen:

- Überprüfen der Voraussetzungen und Hinweise (siehe Seite 204)
- Überprüfen, ob das Hilfsprogramm "d2drestorevol" installiert ist (siehe Seite 205)
- Überprüfen der Volume-Details in der Sitzung (siehe Seite 206)
- Übergeben des Volume-Wiederherstellungsjobs (siehe Seite 207)
- Abbrechen des Volume-Wiederherstellungsjobs (siehe Seite 210)
- Überprüfen des wiederhergestellten Volumes (siehe Seite 210)

Überprüfen der Voraussetzungen und Hinweise

Überprüfen Sie folgende Voraussetzungen, bevor Sie Volumes wiederherstellen:

- Sie haben eine gültige Sicherungssitzung, um eine Wiederherstellung durchzuführen.
- Der Zugriff auf Sicherungssitzungen muss lokal auf dem Zielknoten erfolgen. Wenn der Sitzungsspeicherort auf dem lokalen Volume des Zielknotens ist, verwenden Sie den genauen Verzeichnispfad als Sitzungsspeicherort. Wenn der Sitzungsspeicherort auf einer Netzwerkfreigabe ist, laden Sie zuerst die Netzwerkfreigabe auf einen lokalen Bereitstellungspunkt, und verwenden Sie dann den Pfad des Bereitstellungspunkts als Sitzungsspeicherort.
- Zielvolumes, die Sie wiederherstellen möchten, müssen mithilfe des "umount"-Befehls entladen werden:

  `Beispiel: umount /dev/sda2`
- Das Ziel-Volume muss gleich/größer als das Quell-Volume sein.
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Beachten Sie folgende Hinweise, bevor Sie Volumes wiederherstellen:

- Wenn Sie eine Wiederherstellung durchführen, werden vorhandene Daten auf dem Zielvolume gelöscht. Führen Sie eine Sicherung Ihrer vorhandenen Daten vom Zielvolume aus, bevor Sie die Wiederherstellung durchführen.

Überprüfen, ob das Hilfsprogramm "d2drestorevol" installiert ist

Das d2drestorevol-Hilfsprogramm stellt das Volume auf dem Zielknoten wieder her. Der Zielknoten kann ein Sicherungsserver oder ein anderer Linux-Knoten (Client) sein. Wenn das restorevol-Hilfsprogramm nicht auf dem Zielknoten installiert ist, müssen Sie das Hilfsprogramm manuell installieren.

Wiederherstellung auf einem Sicherungsserver

Wenn der Zielknoten ein Sicherungsserver ist, dann ist das Hilfsprogramm bereits mit dem Installationspaket installiert. Überprüfen Sie, ob das Hilfsprogramm im Ordner "*bin*" vorhanden ist.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Sicherungsserver an.
2. Stellen Sie sicher, dass sich das Hilfsprogramm unter folgendem Speicherort befindet:

   ```
   /opt/CA/d2dserver/bin/d2drestorevol
   ```

   Das Hilfsprogramm wird installiert und überprüft.

Wiederherstellung auf einem Client

Auf einem Client-Knoten ist das Hilfsprogramm nicht installiert. Sie müssen das Hilfsprogramm auf dem Client manuell installieren.

Wichtig! Das Hilfsprogramm muss vom Sicherungsserver, wie in folgenden Schritten beschrieben, heruntergeladen werden. Wenn Sie das Hilfsprogramm von einem Sicherungsserver manuell auf einen Client kopieren, dann wird das Hilfsprogramm möglicherweise nicht richtig funktionieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Client an.
2. Suchen Sie über die Befehlszeile den Download-Pfad für das d2drestorevol-Hilfsprogramm.

   ```
   http[s]://[Backup-Server-address]:[port]/d2drestorevol
   ```

3. Laden Sie das Skript mithilfe eines Befehlszeilentools, wie z. B. "wget", herunter.

   ```
   wget http://192.168.1.1:8014/d2drestorevol –O d2drestorevol
   ```

   Hinweis: Wenn der Server das https-Protokoll verwendet, dann müssen Sie möglicherweise den Parameter "--no-check-certificate" einschließen.

   ```
   wget https://192.168.1.1:8014/d2drestorevol -O d2drestorevol
   --no-check-certificate
   ```

4. Geben Sie die Ausführungsberechtigung für das Hilfsprogramm mithilfe des folgenden Befehls an:

   ```
   chmod +x d2drestorevol
   ```

   Die Berechtigung wird angegeben.

Das Hilfsprogramm "d2drestorevol" wird installiert und überprüft.

Überprüfen der Volume-Details in der Sitzung

Überprüfen Sie die Volume-Details in der Sitzung, die Sie wiederherstellen möchten. Sie können das Quell-Volume, das Dateisystem, die Dateigröße und die Ladeinformationen in der Ausgabe sehen.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Zielknoten an.
2. Verwenden Sie folgenden Befehl, um die Volume-Informationen zu überprüfen:

   ```
   d2drestorevol --command=info --storage-path=<local_path> --node=<node_name>
   --rp=<recovery_point>
   ```

   --command=info

   Gibt an, dass die Volume-Details der Sitzung angezeigt werden.

   --storage-path

   Gibt den Pfad an, der im Thema "Voraussetzungen" festgelegt wurde. Weitere Informationen finden Sie unter "Überprüfen der Voraussetzungen und Hinweise".

--node

Gibt den Quellknoten an, der gesichert wurde.

--rp

Gibt den Wiederherstellungspunkt oder die Wiederherstellungssitzung an, die Sie wiederherstellen möchten. Ein Wiederherstellungspunkt wird üblicherweise im Format "S00000000X" angegeben, wobei "X" für einen numerischen Wert steht.

Die Ausgabe wird angezeigt.

Die Volume-Details werden überprüft.

Übergeben des Volume-Wiederherstellungsjobs

Übergeben Sie den Volume-Wiederherstellungsjob, um mit der Wiederherstellung Ihres Volume auf dem Zielknoten zu beginnen.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Zielknoten an.
2. Übergeben Sie den Wiederherstellungsjob mithilfe des folgenden Befehls:

```
d2drestorevol --command=restore  --storage-path=<lokaler_Pfad>
--node=<Knotenname> --rp=<Wiederherstellungspunkt>
--source-volume=<Quell-Volume> --target-volume=<Ziel-Volume>
[--encryption-password=<Verschlüsselungskennwort>]
[--mount-target=<Ladepunkt> [--quick-recovery]]
```

--command=restore

Gibt an, dass der Volume-Wiederherstellungsjob übergeben wurde.

--storage-path

Gibt den Pfad an, der im Thema "Voraussetzungen" festgelegt wurde. Weitere Informationen finden Sie unter "Überprüfen der Voraussetzungen und Hinweise".

--node

Gibt den Quellknoten an, der gesichert wurde.

--rp

Gibt den Wiederherstellungspunkt bzw. die Wiederherstellungssitzung an, die Sie wiederherstellen möchten. Ein Wiederherstellungspunkt wird üblicherweise im Format "S00000000X" angegeben, wobei "X" für einen numerischen Wert steht.

--encryption-password

Gibt das Sitzungskennwort an. Diese Option ist erforderlich, wenn die Sitzung verschlüsselt ist. Wenn die Sitzung verschlüsselt und diese Option nicht vorhanden ist, werden Sie aufgefordert, das Kennwort über den Terminal einzugeben.

--source-volume

Gibt das Quell-Volume an. Sie können das Quell-Volume mithilfe des Parameters "*command=info*" abrufen, wie unter dem Abschnitt "Überprüfen der Volume-Details in der Sitzung" beschrieben, oder das Quell-Volume kann der Bereitstellungspunkt des Quellsystems sein.

--target-volume

Gibt den Gerätedateipfad des Zielknotens an.

Beispiel: /dev/sda2

--mount-target

Gibt den Bereitstellungspunkt an, an dem das wiederhergestellte Volume geladen werden soll.

Beispiel: /mnt/volrestore

--quick-recovery

Wenn dies gemeinsam mit "--mount-target" verwendet wird, wird der Zieldatenträger so schnell wie möglich geladen. Sie können die Daten auf dem Zieldatenträger verwenden, während die Daten wiederhergestellt werden.

Nachdem der Wiederherstellungsjob abgeschlossen ist, wird die Wiederherstellung automatisch beendet, und Sie können ohne Unterbrechung damit fortfahren, die Daten zu verwenden.

Hinweis: Bei gleichzeitiger Ausführung eines Volume-Wiederherstellungsjob und eines Sicherungsjobs:

- Wenn "--quick-recovery" verwendet wird, wird jener Job (Volume-Wiederherstellung oder Sicherung), der später gestartet wird, nicht ausgeführt.
- Wenn "--quick-recovery" nicht verwendet wird, sichert der Sicherungsjob nur jene Volumes, die nicht wiederhergestellt werden.

Der Wiederherstellungsjob wird übergeben, und es wird ein Fenster geöffnet, das den Fortschritt anzeigt. Wenn Sie andere Jobs übergeben möchten, können Sie entweder warten, bis der aktuelle Job abgeschlossen ist, oder Sie können auf "Q" drücken, um das Fenster zu verlassen und anschließend einen neuen Job übergeben.

3. (Optional) Verwenden Sie folgenden Befehl, um den Fortschritt des Volume-Wiederherstellungsjobs zu verfolgen:

   ```
   d2drestorevol --command=monitor
   ```

   Die Fortschrittsdetails, wie z. B. Volumename, vergangene Zeit, Fortschritt, Geschwindigkeit, Status und verbleibende Zeit, werden in einem Fenster angezeigt.

   Das Fenster wird verlassen, wenn der Job fertiggestellt wird. Sie können auch auf "Q" drücken, um das Fenster manuell zu verlassen. Das manuelle Schließen des Fensters unterbricht die Ausführung des Wiederherstellungsjobs nicht.

Der Volume-Wiederherstellungsjob wird übergeben.

Abbrechen des Volume-Wiederherstellungsjobs

Sie können den Volume-Wiederherstellungsjob von der Befehlszeile des Zielknotens abbrechen. Verwenden Sie folgenden Befehl, um den Volume-Wiederherstellungsjob abzubrechen.

```
d2drestorevol --command=cancel --target-volume=<target_volume>
```

--command=cancel

Gibt an, dass der Volume-Wiederherstellungsjob abgebrochen wurde.

--target-volume

Gibt den Gerätedateipfad des Zielknotens an. Der Wert muss identisch mit dem Wert sein, der verwendet wird, um den Wiederherstellungsjob zu übergeben.

Wichtig: Wenn Sie einen Volume-Wiederherstellungsjob abbrechen, wird das Zielvolume unbrauchbar. In solchen Fällen können Sie erneut versuchen, den Volume-Wiederherstellungsjob auszuführen, oder Sie können die verlorenen Daten wiederherstellen, wenn Sie eine Sicherung haben.

Überprüfen des wiederhergestellten Volumes

Überprüfen Sie die Daten, wenn das Volume wiederhergestellt ist.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Zielknoten an.
2. Überprüfen Sie das Fortschrittsfenster, um den Abschlussstatus zu prüfen.

3. (Optional) Überprüfen Sie die Datei "*d2drestvol_activity_[target-volume].log*", um alle Protokolle des Wiederherstellungsjobs anzuzeigen.
4. Laden Sie das wiederhergestellte Volume, und überprüfen Sie, ob die Daten wiederhergestellt sind.

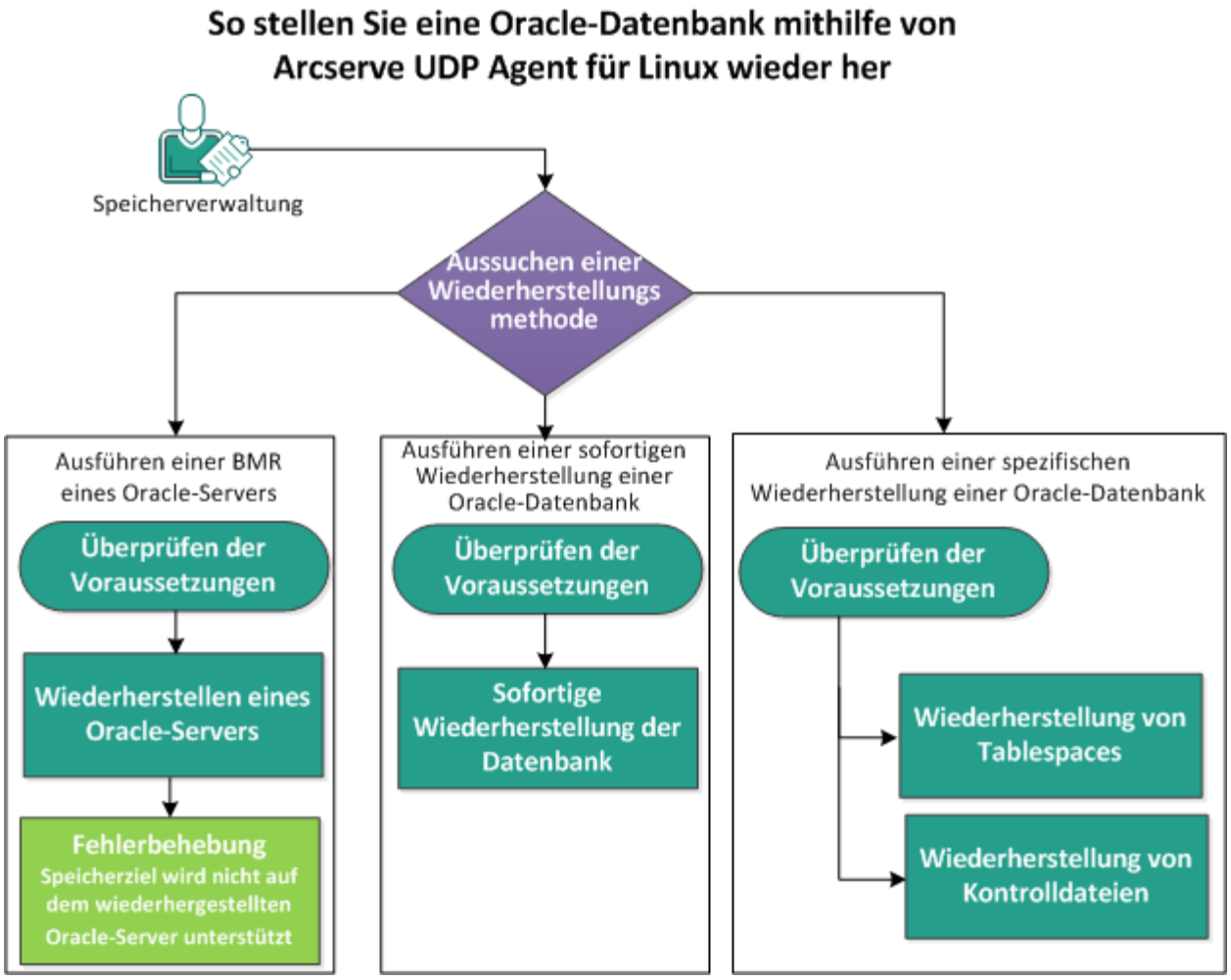
   Der Volume-Wiederherstellungsjob ist überprüft.

Das Volume wurde erfolgreich wiederhergestellt.

So stellen Sie eine Oracle-Datenbank mithilfe von Arcserve UDP Agent (Linux) wieder her

Sie können die gesamte Oracle-Datenbank oder spezifische Dateien von der Datenbank wiederherstellen. Sie können auch eine Bare-Metal-Recovery (BMR) eines Oracle-Servers ausführen, wenn der Quellserver nicht richtig funktioniert. Wenn Sie die Datenbank verloren haben und sie sofort verfügbar sein soll, können Sie eine sofortige Wiederherstellung ausführen. Lesen Sie die Voraussetzungen für jeden Wiederherstellungstyp, bevor Sie mit der Wiederherstellung beginnen.

Das folgende Diagramm veranschaulicht den Prozess zum Wiederherstellen einer Oracle-Datenbank mithilfe von Arcserve UDP Agent (Linux):


So stellen Sie eine Oracle-Datenbank mithilfe von Arcserve UDP Agent für Linux wieder her
Speicherverwaltung
Aussuchen einer Wiederherstellungs methode
Ausführen einer BMR eines Oracle-Servers
Überprüfen der Voraussetzungen
Wiederherstellen eines Oracle-Servers
Fehlerbehebung
Speicherziel wird nicht auf dem wiederhergestellten Oracle-Server unterstützt
Ausführen einer sofortigen Wiederherstellung einer Oracle-Datenbank
Überprüfen der Voraussetzungen
Sofortige Wiederherstellung der Datenbank
Ausführen einer spezifischen Wiederherstellung einer Oracle-Datenbank
Überprüfen der Voraussetzungen
Wiederherstellung von Tablespaces
Wiederherstellung von Kontrolldateien

Führen Sie folgende Schritte aus, um eine Oracle-Datenbank mithilfe von Arcserve UDP Agent (Linux) wiederherzustellen:

- Ausführen einer BMR eines Oracle-Servers (siehe Seite 213)
- Ausführen einer sofortigen Wiederherstellung einer Oracle-Datenbank (siehe Seite 215)
- Ausführen einer spezifischen Wiederherstellung einer Oracle-Datenbank (siehe Seite 217)

Ausführen einer Bare-Metal-Recovery (BMR) eines Oracle-Servers

Eine BMR stellt das Betriebssystem und die Software-Anwendungen sowie alle gesicherten Daten wieder her. Eine BMR ist der Prozess, bei dem ein Bare-Metal-Computersystem wiederhergestellt wird. "Bare Metal" bezeichnet einen Computer ohne Betriebssystem, Treiber und Software-Anwendungen. Nachdem die Wiederherstellung abgeschlossen wurde, startet der Zielcomputer automatisch in der gleichen Betriebsumgebung wie der Sicherungsquellknoten neu, und alle Daten werden wiederhergestellt.

Sie können eine BMR unter Verwendung der IP-Adresse oder der MAC-Adresse (Media Access Control) des Zielcomputers ausführen. Wenn Sie den Zielcomputer mithilfe der Arcserve UDP Agent (Linux)-Live-CD booten, können Sie die IP-Adresse des Zielcomputers abrufen.

Überprüfen der Voraussetzungen

Überprüfen Sie die folgenden Voraussetzungen, bevor Sie die Oracle-Datenbank wiederherstellen:

- Sie verfügen über einen gültigen Wiederherstellungspunkt und, falls erforderlich, über das Verschlüsselungskennwort für die Wiederherstellung.
- Sie verfügen über einen gültigen Zielcomputer für die BMR.
- Sie haben die Arcserve UDP Agent (Linux)-(Linux-)Live-CD erstellt.
- Wenn Sie eine BMR mithilfe der IP-Adresse ausführen möchten, müssen Sie die IP-Adresse des Zielcomputers mithilfe der Live-CD abrufen.
- Wenn Sie eine PXE-basierte BMR mithilfe der MAC-Adresse ausführen möchten, müssen Sie die MAC-Adresse des Zielcomputers haben.
- Oracle-Datenbank speichert alle datenbankbezogenen Dateien (Datendateien, Redo-Protokolle, Archivprotokolle, pfile, spfile, Sicherungen) auf ext2, ext3, ext4 und ReiserFS. Die Datenbank erkennt keine Oracle Cluster-Dateisysteme (OCFS/OCFS2), rohe Datenträger oder ASM-Dateisysteme (Automatic Storage Management).
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Wiederherstellen eines Oracle-Servers

Wenn der Oracle-Server beschädigt ist, können Sie den gesamten Server wiederherstellen, indem Sie eine BMR ausführen.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer bei der Konsole des Linux-Sicherungsservers.

2. Führen Sie eine BMR mithilfe des Wiederherstellungs-Assistenten aus. Weitere Informationen zur Wiederherstellung finden Sie unter "So führen Sie eine Bare-Metal-Recovery (BMR) für Linux-Rechner aus".
3. Nachdem der BMR-Job abgeschlossen ist, melden Sie sich beim Zielcomputer an, und überprüfen Sie, ob die Datenbank wiederhergestellt ist.

Der Oracle-Server ist erfolgreich wiederhergestellt.

Speicherziel wird nicht auf dem wiederhergestellten Oracle-Server unterstützt

Symptom:

Ich habe eine Bare-Metal-Recovery eines Oracle-Servers ausgeführt. Die Speichergröße des Zielcomputers ist weniger als der Quellen-Oracle-Server, und die Oracle-Datenbank verwendet AMM (Automatic Memory Management). Wenn ich nach der BMR die Oracle-Datenbankinstanz starte, dann erhalte ich folgenden Fehler:

SQL> startup

ORA-00845: MEMORY_TARGET not supported on this system

Lösung:

Um diesen Fehler zu beheben, vergrößern Sie den gemeinsamen Speicher des virtuellen Dateisystems.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Zielrechner an.
2. Öffnen Sie die Eingabeaufforderung, und überprüfen Sie die Größe des gemeinsamen Speichers des virtuellen Dateisystems.

```
# df -k /dev/shm
Filesystem           1K-blocks      Used Available Use% Mounted on
tmpfs                   510324        88    510236   1% /dev/shm
```

3. Geben Sie folgenden Befehl ein, und geben Sie die erforderliche Größe des gemeinsamen Speichers an:
```
# mount -o remount,size=1200m /dev/shm
```
4. Navigieren Sie zum Ordner "/etc/fstab", und aktualisieren Sie die tmpfs-Einstellung:
```
tmpfs /dev/shm tmpfs size=1200m 0 0
```

Hinweis: Der gemeinsame Speicher des virtuellen Dateisystems sollte groß genug sein, um die Werte MEMORY_TARGET und MEMORY_MAX_TARGET unterzubringen. Weitere Informationen zu den Variablen finden Sie in der Oracle-Dokumentation.

Ausführen einer sofortigen Wiederherstellung einer Oracle-Datenbank

Sie können eine Oracle-Datenbank sofort wiederherstellen, ohne eine vollständige BMR auszuführen. Sie können die Datenbank wiederherstellen, indem Sie bestimmte Befehle in der Befehlszeile verwenden.

Überprüfen der Voraussetzungen

Überprüfen Sie die folgenden Voraussetzungen, bevor Sie die Oracle-Datenbank wiederherstellen:

- Sie verfügen über einen gültigen Wiederherstellungspunkt und, falls erforderlich, über das Verschlüsselungskennwort für die Wiederherstellung.
- Der Zugriff auf Sicherungssitzungen muss lokal auf dem Zielknoten erfolgen. Wenn der Sitzungsspeicherort auf dem lokalen Volume des Zielknotens ist, verwenden Sie den genauen Verzeichnispfad als Sitzungsspeicherort. Wenn der Sitzungsspeicherort auf einer Netzwerkfreigabe ist, laden Sie zuerst die Netzwerkfreigabe auf einen lokalen Bereitstellungspunkt, und verwenden Sie dann den Pfad des Bereitstellungspunkts als Sitzungsspeicherort.
- Ziel-Volumens, die Sie wiederherstellen möchten, dürfen keine Root-Volumes sein und müssen mithilfe des "umount"-Befehls entladen werden.

  Beispiel: umount /dev/sda1
- Das Ziel-Volume muss gleich/größer als das Quell-Volume sein.
- Oracle-Datenbank speichert alle datenbankbezogenen Dateien (Datendateien, Redo-Protokolle, Archivprotokolle, pfile, spfile, Sicherungen) auf ext2, ext3, ext4 und ReiserFS. Die Datenbank erkennt keine Oracle Cluster-Dateisysteme (OCFS/OCFS2), rohe Datenträger oder ASM-Dateisysteme (Automatic Storage Management).
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Sofortige Wiederherstellung der Datenbank

Wenn Sie die Datenbank sofort wiederherstellen, dann ist die Datenbank zur sofortigen Verwendung verfügbar. Allerdings wird die Wiederherstellung im Backend ausgeführt, und alle Dateien sind erst verfügbar, nachdem die Datenbank vollständig wiederhergestellt wurde.

Hinweis: Weitere Informationen zur Volume-Wiederherstellung finden Sie unter "So stellen Sie Volumes auf einem Zielknoten wieder her".

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Zielrechner an.
2. Öffnen Sie als root-Benutzer eine Eingabeaufforderung.
3. Stellen Sie sicher, dass der Zieldatenträger "/dev/sdb1" nicht geladen ist.
   ```
   # df | grep ‘target_volume’
   ```
   Beispiel: # df | grep '/dev/sdb1'
4. Laden Sie die Remote-NFS-Freigabe in den lokalen Pfad.
   ```
   #mount <nfs_session_path>:/nfs  <session_location_on_local>
   ```
   Example: #mount xxx.xxx.xxx.xxx:/nfs /CRE_ROOT
5. Geben Sie folgenden Befehl ein, um den Wiederherstellungsjob zu starten:
   ```
   #. /d2drestorevol --command=restore --storage-path=<session_location_on_local>
   --node=<oracle_server> --rp=last
   --source-volume=<mount_point_for_oracle_data_volume>
   --target-volume=<restore_target_volume_name>
   --mount-target=<mount_point_for_oracle_data_volume> --quick-recovery
   ```
   Beispiel: #. /d2drestorevol --command=restore --storage-path=/CRE_ROOT --node=rh63-v2 --rp=last --source-volume=/opt/oracle --target-volume=/dev/sdb1 --mount-target=/opt/oracle --quick-recovery

   Sie können die Oracle-Datenbank sofort starten, nachdem der Wiederherstellungsjob gestartet wurde. Sie müssen nicht auf den Abschluss der Datenbankwiederherstellung warten.
6. Öffnen Sie eine weitere Eingabeaufforderung, und melden Sie sich mit dem Oracle-Benutzernamen und -Kennwort an.
   ```
   $sqlplus / as sysdba
   SQL>startup;
   ```
   Die Oracle-Datenbank wird geöffnet, und Sie können die normalen Datenbankvorgänge ausführen, wie z. B. Daten abfragen, einfügen, löschen, aktualisieren usw.

Die Oracle-Datenbank wird sofort wiederhergestellt.

Ausführen einer spezifischen Wiederherstellung einer Oracle-Datenbank

Sie können bestimmte Dateien wiederherstellen, die mit der Oracle-Datenbank verknüpft sind. Diese Dateien können Kontrolldateien oder Datendateien von Tablespaces sein.

Überprüfen der Voraussetzungen

Überprüfen Sie die folgenden Voraussetzungen, bevor Sie die Oracle-Datenbank wiederherstellen:

- Sie verfügen über einen gültigen Wiederherstellungspunkt und, falls erforderlich, über das Verschlüsselungskennwort.
- Sie verfügen über einen gültigen Zielknoten zum Wiederherstellen der Daten.
- Sie haben sichergestellt, dass der Linux-Sicherungsserver das Dateisystem unterstützt, das Sie wiederherstellen möchten.
- Oracle-Datenbank speichert alle datenbankbezogenen Dateien (Datendateien, Redo-Protokolle, Archivprotokolle, pfile, spfile, Sicherungen) auf ext2, ext3, ext4 und ReiserFS. Die Datenbank erkennt keine Oracle Cluster-Dateisysteme (OCFS/OCFS2), rohe Datenträger oder ASM-Dateisysteme (Automatic Storage Management).
- Überprüfung Sie die Kompatibilitätsmatrix, welche die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Wiederherstellung von Tablespaces

Wenn ein Datenbank-Tablespace verloren oder beschädigt ist, können Sie es wiederherstellen, indem Sie eine Wiederherstellung auf Dateiebene ausführen. Nachdem die Wiederherstellung auf Dateiebene erfolgreich gewesen ist, müssen Sie den Tablespace manuell wiederherstellen.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Zielrechner an.
2. Stellen Sie sicher, dass die Datenbank verfügbar ist.

3. Stellen Sie den erforderlichen Tablespace offline.

   Beispiel: Angenommen, der Name des Tablespace ist "MYTEST_DB". Geben Sie folgenden Befehl ein, um den Tablespace offline zu stellen:

   ```
   $ sqlplus "/ as sysdba"
   SQL> alter tablespace MYTEST_DB offline;
   ```

4. Listet alle Datendateien für den angegebenen Tablespace "MYTEST_DB" auf.

   ```
   SQL> select file_name, tablespace_name from dba_data_files where
   tablespace_name='MYTEST_DB';

   FILE_NAME

   --------------------------------------------------------------------------------
   ---

   TABLESPACE_NAME

   ------------------------------

   /opt/oracle/oradata/lynx/MYTEST_DATA01.dbf

   MYTEST_DB
   ```

5. Stellen Sie die Datendateien von Tablespaces mithilfe des Wiederherstellungs-Assistenten wieder her. Weitere Informationen zur Wiederherstellung finden Sie unter "So führen Sie eine Wiederherstellung der Dateiebene unter Linux-Knoten aus".

6. Geben Sie folgende Informationen im Wiederherstellungs-Assistenten an, und übergeben Sie den Job:

   a. Wenn Sie die Dateien und Ordner auswählen, geben Sie den erforderlichen Datendateinamen des Tablespace ein, und suchen Sie ihn.

      Beispiel: Geben Sie "MYTEST_DATA01.dbf" des Tablespace "MYTEST_DB" ein, und suchen Sie ihn.

   b. Geben Sie auf der Seite "Zielcomputer" die folgenden Informationen ein:

      - Wählen Sie "Am ursprünglichen Speicherort wiederherstellen" aus.
      - Geben Sie den Hostnamen oder die IP-Adresse des Oracle-Zielservers ein.
      - Geben Sie den root-Benutzernamen und das Kennwort des Oracle-Zielservers ein.
      - Wählen Sie die Option "Overwrite existing files for the Resolving Conflicts" (Vorhandene Dateien für die Konfliktlösung überschreiben) aus.

7. Nachdem die Datendatei wiederhergestellt wurde, stellen Sie den Tablespace der Oracle-Datenbank wieder her.

```
SQL>recover tablespace MYTEST_DB;
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
Auto
```

8. Stellen Sie den angegebenen Tablespace online.

```
SQL>alter tablespace MYTEST_DB online;
```

Der Tablespace wurde erfolgreich wiederhergestellt.

Wiederherstellung von Kontrolldateien

Wenn Datenbank-Kontrolldateien verloren oder beschädigt sind, können Sie sie wiederherstellen, indem Sie eine Wiederherstellung auf Dateiebene ausführen. Nachdem die Wiederherstellung auf Dateiebene erfolgreich gewesen ist, müssen Sie die Kontrolldateien manuell wiederherstellen.

Gehen Sie wie folgt vor:

1. Melden Sie sich als root-Benutzer beim Zielrechner an.
2. Fahren Sie die Oracle-Instanz herunter.

```
SQL>shutdown abort
```

3. Starten Sie die Datenbank im "nomount"-Status.

```
SQL>startup nomount
```

4. Listet den Pfad für alle Kontrolldateien auf.

```
SQL> show parameter control_files;
NAME                                 TYPE        VALUE
------------------------------------ -----------
------------------------------
control_files               string    /opt/oracle/oradata/lynx/control01.ctl,
/opt/oracle/flash_recovery_area/lynx/control02.ctl
```

5. Stellen Sie die Kontrolldateien mithilfe des Wiederherstellungs-Assistenten wieder her. Weitere Informationen zur Wiederherstellung finden Sie unter "So führen Sie eine Wiederherstellung der Dateiebene unter Linux-Knoten aus".

6. Geben Sie folgende Informationen im Wiederherstellungs-Assistenten an, und übergeben Sie den Job:

   a. Wenn Sie die Dateien und Ordner auswählen, geben Sie den erforderlichen Namen de Kontrolldatei ein, und suchen Sie sie. Wiederholen Sie diesen Schritt, bis alle Kontrolldateien ausgewählt sind.

      Beispiel: Geben "control01.ctl " ein, und suchen Sie sie.

   b. Geben Sie auf der Seite "Zielcomputer" die folgenden Informationen ein:

      - Wählen Sie "Am ursprünglichen Speicherort wiederherstellen" aus.
      - Geben Sie den Hostnamen oder die IP-Adresse des Oracle-Zielservers ein.
      - Geben Sie den root-Benutzernamen und das Kennwort des Oracle-Zielservers ein.
      - Wählen Sie die Option "Overwrite existing files for the Resolving Conflicts" (Vorhandene Dateien für die Konfliktlösung überschreiben) aus.

7. Nachdem alle Kontrolldateien wiederhergestellt sind, laden Sie die Datenbank, und öffnen Sie sie.

   ```
   $sqlplus / as sysdba
   SQL>alter database mount;
   ```

8. Stellen Sie die Datenbank mit dem "RECOVER"-Befehl wieder her, und fügen Sie die "USING BACKUP CONTROLFILE"-Klausel hinzu.

   ```
   SQL> RECOVER DATABASE USING BACKUP CONTROLFILE
   ```

9. Wenden Sie die aufgeforderten archivierten Protokolle an.

   Hinweis: Wenn das erforderliche archivierte Protokoll fehlt, dann bedeutet dies, dass sich ein notwendiger Redo-Datensatz in den Online-Redo-Protokollen befindet. Dies tritt auf, weil sich unarchivierte Änderungen in den Online-Protokollen befinden, als die Instanz fehlgeschlagen ist. Sie können den vollständigen Pfad einer Online-Redo-Protokolldatei angeben, und drücken Sie die Eingabetaste (möglicherweise müssen Sie dies ein paar Mal probieren, bis Sie das richtige Protokoll finden).

   Beispiel:

   ```
   SQL> RECOVER DATABASE USING BACKUP CONTROLFILE
   ORA-00279: change 1035184 generated at 05/27/2014 18:12:49 needed for thread 1
   ORA-00289: suggestion :
   /opt/oracle/flash_recovery_area/LYNX/archivelog/2014_05_27/o1_mf_1_6_%u_.arc
   ORA-00280: change 1035184 for thread 1 is in sequence #6
   Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
   /opt/oracle/oradata/lynx/redo03.log
   Log applied.
   Media recovery complete.
   ```

10. Öffnen Sie die Datenbank mit der RESETLOGS-Klausel, nachdem Sie den Wiederherstellungsprozess abgeschlossen haben.

    ```
    SQL>alter database open resetlogs;
    ```

Die Kontrolldateien sind erfolgreich wiederhergestellt.

Kapitel 5: Fehlerbehebung

Dieses Kapitel enthält folgende Themen:

Arcserve UDP Agent (Linux) kann nicht auf unterstützten Servern installiert werden (siehe Seite 224)
Arcserve UDP Agent (Linux) zeigt einen Zeitlimitfehler des Vorgangs an (siehe Seite 225)
Alle geplanten Jobs schlagen fehl, wenn die Systemzeit auf einen bereits vergangenen Wert geändert wird (siehe Seite 226)
Arcserve UDP Agent (Linux) konnte Linux Software RAID-Geräte nicht bereitstellen (siehe Seite 226)
Eine sogenannte Paravirtual Machine (PVM) zeigt einen schwarzen Bildschirm auf dem Fenster des Virtual Network Computing (VNC) Client an, wenn mithilfe einer Live-CD gestartet wird (siehe Seite 227)
So stellen Sie nach einem BMR-Job auf einem Oracle VM-Server die Datenträger-Boot-Sequenz ein (siehe Seite 228)
Der Sicherungsjob schlägt beim Erfassen der mit BMR verbundenen Informationen fehl, oder der BMR-Job schlägt dabei fehl, ein Datenträger-Layout zu erstellen (siehe Seite 230)
Der Sicherungs-Lesedurchsatz ist geringer, wenn der Sicherungsknoten RHEL, CentOS oder Oracle Linux 5.x auf einer Xen- basierten PVM ist. (siehe Seite 231)
So stellen Sie die Vorgängerversion des Sicherungsservers wieder her (siehe Seite 232)
SLES 10.X startet nach einer BMR nicht erfolgreich (siehe Seite 233)
d2drestorevm- und d2dverify-Jobs schlagen auf Oracle VM Server fehl (siehe Seite 233)
Der virtuelle ESXi-Rechner kann nach einer BMR von einem physischen Rechner nicht gestartet werden (siehe Seite 234)

Arcserve UDP Agent (Linux) kann nicht auf unterstützten Servern installiert werden

Gültig unter CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, SUSE Linux Enterprise Server (SLES) 11.x und Oracle Linux Server 6.x

Problem

Wenn ich Arcserve UDP Agent (Linux) installiere, schlägt die Installation mit folgenden Linux-Warnmeldungen fehl:

```
mkisofs         Create Live CD image

mount.nfs               Mount NFS share file system as backup destination and restore
source

mount.cifs              Mount CIFS share file system as backup destination and
restore source

The following processes must be running

Inactive Processes              Affected Function

rpc.statd               The NFS file locking function does not work
```

Lösung

Bei Beginn der Installation überprüft Arcserve UDP Agent (Linux), ob das Linux-BS die Anforderungen des Sicherungsservers erfüllt. Wenn das Linux-BS die Mindestanforderungen nicht erfüllt, zeigt Arcserve UDP Agent (Linux) eine Warnmeldung an, um Sie auf dieses Problem hinzuweisen. Die Meldung umfasst die Liste aller Pakete, die für den Sicherungsserver erforderlich sind.

Um dieses Arcserve UDP Agent (Linux)-Installationsproblem zu beheben, führen Sie folgende Schritte aus:

1. Installieren Sie folgende Pakete mithilfe des *yum*-Befehls:
   - genisoimage
   - nfs-utils
   - cifs-utils
2. Führen Sie die folgenden zwei Befehle aus:

   ```
   service rpcbind start

   service nfs start
   ```
3. Führen Sie folgenden Befehl aus, um sicherzustellen, dass *rpc.statd* ausgeführt wird:

   ```
   ps -ef|grep rpc.statd
   ```
4. Installieren Sie Arcserve UDP Agent (Linux) neu.

Arcserve UDP Agent (Linux) wurde erfolgreich installiert.

Arcserve UDP Agent (Linux) zeigt einen Zeitlimitfehler des Vorgangs an

Gültig unter CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, SUSE Linux Enterprise Server (SLES) 11.x und Oracle Linux Server 6.x

Problem

Ich erhalte folgende Fehlermeldung:

Der Vorgang hat das Zeitlimit überschritten. Die maximale Dauer zum Abschluss des Vorgangs wurde überschritten. Versuchen Sie es später erneut.

Ich erhalte diese Meldung häufig, wenn ich eine Wiederherstellung auf Dateiebene ausführe und durch Wiederherstellungspunkte navigiere, die mehr als 1.000 inkrementelle Wiederherstellungspunkte haben.

Lösung

Der Standardwert für das Zeitlimit beträgt 3 Minuten. Sie können das Problem beheben, indem Sie den Wert für das Zeitlimit vergrößern.

Führen Sie folgende Schritte aus, um den Wert für das Zeitlimit zu vergrößern:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Fügen Sie folgende Systemumgebungsvariable hinzu:

   `D2D_WEBSVR_TIMEOUT`

   Der Wert für die Umgebungsvariable ist eine Zahl. Die Zahl muss größer als 3 sein. Die Einheit für den Wert wird in Minuten angegeben.
3. Starten Sie den Sicherungsserver neu.

Der Wert für das Zeitlimit ist erfolgreich vergrößert.

Alle geplanten Jobs schlagen fehl, wenn die Systemzeit auf einen bereits vergangenen Wert geändert wird

Gültig unter CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, SUSE Linux Enterprise Server (SLES) 11.x und Oracle Linux Server 6.x

Problem

Wenn ich die Systemzeit in einen bereits vergangenen Wert ändere, dann sind alle meine geplanten Jobs betroffen. Die geplanten Jobs können nicht ausgeführt werden, nachdem ich die Systemzeit in einen früheren Zeitpunkt geändert habe.

Lösung

Nachdem Sie die Systemzeit geändert haben, starten Sie den Sicherungsdienst neu.

Führen Sie diese Schritte aus, um den Sicherungsdienst neu zu starten:

1. Melden Sie sich als root-Benutzer beim Sicherungsserver an.
2. Wechseln Sie in den bin-Ordner

   ```
   /opt/CA/d2dserver/bin/
   ```

3. Starten Sie den Sicherungsserver mit folgendem Befehl neu:

   ```
   d2dserver restart
   ```

   Der Sicherungsserver wird neu gestartet.

Alle geplanten Jobs werden nach Ablaufplan ausgeführt.

Arcserve UDP Agent (Linux) konnte Linux Software RAID-Geräte nicht bereitstellen

Gültig unter CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, SUSE Linux Enterprise Server (SLES) 11.x und Oracle Linux Server 6.x

Problem

Manchmal kann der BMR-Prozess Linux-Software-RAID-Geräte nicht mounten, nachdem der Zielcomputer neu gestartet wurde.

Lösung

Um dieses Problem zu lösen, starten Sie Ihren Zielcomputer neu.

Eine sogenannte Paravirtual Machine (PVM) zeigt einen schwarzen Bildschirm auf dem Fenster des Virtual Network Computing (VNC) Client an, wenn mithilfe einer Live-CD gestartet wird

Gültig auf PVM unter Oracle VM Server

Problem

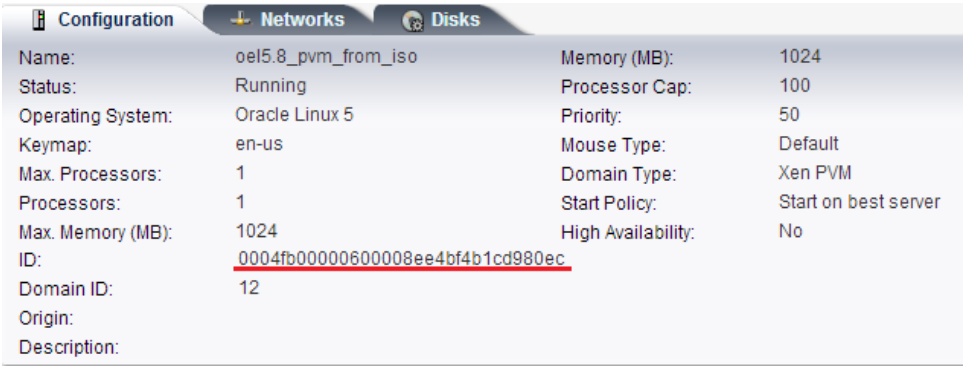
Auf einem Oracle VM Server wird, wenn ich die Paravirtual Machine (PVM) mithilfe einer Live-CD starte, ein schwarzer Bildschirm auf dem VNC Client-Fenster angezeigt.

Lösung

Um dieses Problem zu lösen, melden Sie sich vom Backend aus bei der Live-CD-Konsole an.

Gehen Sie wie folgt vor:

1. Starten Sie die VM mithilfe einer Live-CD.
2. Notieren Sie die ID der VM, auf die Sie von Oracle VM Manager aus zugreifen können.



3. Melden Sie sich mithilfe der Secure Shell (SSH) bei dem Oracle VM-Server an, auf dem die VM ausgeführt wird.
4. Führen Sie den Befehl *xm console $ID* aus, wie im folgenden Diagramm gezeigt:

```
[root@                ~]# xm console 0004fb00000600008ee4bf4b1cd980ec
```

5. (Optional) Drücken Sie die Eingabetaste, wenn Sie aufgefordert werden, den Vorgang zu bestätigen.
6. Die Konsole der mit der Live-CD gestarteten Xen PVM wird geöffnet.
7. Konfigurieren Sie das Netzwerk.
8. Verlassen Sie die Konsole durch Drücken von STRG+] oder STRG+5.

Das Problem wird gelöst.

So stellen Sie nach einem BMR-Job auf einem Oracle VM-Server die Datenträger-Boot-Sequenz ein

Gültig auf Oracle VM-Server

Problem

Wenn ich einen BMR-Job an einem Zielknoten auf einem Oracle VM-Server ausführe, bekomme ich den folgenden Warnhinweis im Aktivitätsprotokoll:

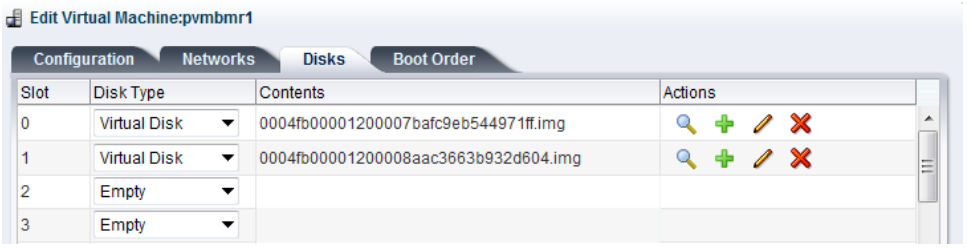
```
Das Startvolume wurde auf dem Datenträger /dev/xxx wiederhergestellt. Passen Sie die Startsequenz des Datenträgers in BIOS an, so dass von /dev/xxx aus gestartet wird.
```

Lösung

Um dieses Problem zu vermeiden, tauschen Sie die Datenträger-Boot-Sequenz des BMR-Zielknotens aus.

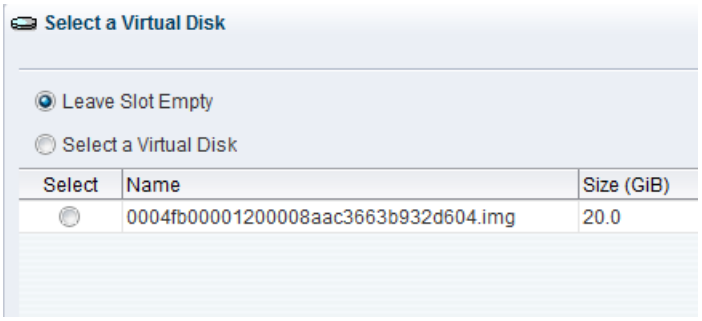
Gehen Sie wie folgt vor:

1. Bearbeiten Sie den BMR-Zielknoten in Oracle VM Manager und klicken auf die Registerkarte "Datenträger".

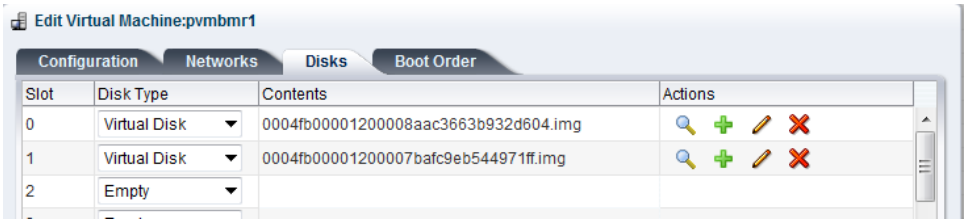


2. Wählen Sie den Datenträger Slot N als den Startdatenträger aus.
3. Notieren Sie den Datenträgernamen und die Slot-Nummer N.

   Sie werden den Datenträgernamen und die Slot-Nummer in späteren Schritten benötigen.
4. Wählen Sie in der Spalte "Aktion" die Schaltfläche "Virtual Machine Disk" aus.
5. Wählen Sie die Option "Leave Slot Empty" und klicken Sie auf "Speichern".



6. Wählen Sie den Datenträger Slot 0 aus und notieren Sie sich den Datenträgernamen.
7. Wählen Sie in der Spalte "Aktion" die Schaltfläche "Virtual Machine Disk" aus.
8. Wählen Sie die Option "Leave Slot Empty" und klicken Sie auf "Speichern".
9. Hängen Sie das ausgewählte Startdatenträger-Image an Slot 0 und das ursprüngliche Startdatenträger-Image von Slot 0 an Slot N an.



10. Starten Sie den BMR-Zielknoten.

Die Datenträger-Boot-Sequenz wurde erfolgreich eingestellt.

Der Sicherungsjob schlägt beim Erfassen der mit BMR verbundenen Informationen fehl, oder der BMR-Job schlägt dabei fehl, ein Datenträger-Layout zu erstellen

Gültig auf Oracle VM Server für HVM mit LVM-Volume

Problem

Wenn ich einen Sicherungsjob für ein HVM mit LVM-Volumes unter einem Oracle VM-Server ausführe, schlägt der Sicherungsjob beim Erfassen der mit BMR verbundenen Informationen fehl. Auch wenn ich einen BMR-Job für ein HVM mit LVM-Volumes unter einem Oracle VM-Server ausführe, schlägt der BMR-Job beim Erstellen des Datenträgerlayouts fehl.

Lösung

Um dieses Problem zu lösen, deaktivieren Sie die PV-Treiber für den Sicherungsquellenknoten.

Gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster zur Eingabeaufforderung auf dem Sicherungsquellenknoten, und geben Sie folgenden Befehl ein:

   ```
   sfdisk –s
   ```

2. Überprüfen Sie, ob der gleiche Datenträger zweimal im Ergebnis angezeigt wird.

   Zum Beispiel sind xvdX und hdX der gleiche Datenträger. Überprüfen Sie, ob beide diese Datenträger im Ergebnis angezeigt werden.

3. Wenn ja, dann führen Sie die folgenden Schritte aus:

   a. Fügen Sie die folgende Zeile zur Datei */etc/modprobe.d/blacklist* auf dem Sicherungsquellenknoten hinzu:

      ```
      blacklist xen_vbd
      ```

   b. Starten Sie den Sicherungsquellenknoten neu und wiederholen Sie den Sicherungsjob.

      Der Sicherungsjob wird ausgeführt.

4. Wenn nein, setzen Sie sich mit dem CA-Support-Team in Verbindung.

Das Problem wird gelöst.

Der Sicherungs-Lesedurchsatz ist geringer, wenn der Sicherungsknoten RHEL, CentOS oder Oracle Linux 5.x auf einer Xen- basierten PVM ist.

Gültig unter Red Hat Enterprise Linux (RHEL), CentOS, SUSE Linux Enterprise Server (SLES) 11.x und Oracle Linux Server 6.x auf Xen-basierten PVMs

Problem

Beim Sichern eines RHEL-, CentOS-, SLES- oder Oracle Linux 6.x-Servers auf einer Xen-basierten PVM ist der Wert der Sicherungs-Lesedurchsatzes niedriger.

Lösung

Um dieses Problem zu lösen, konfigurieren Sie den Datenträgereingabe/-ausgabe-Planer der VM.

Gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster für die Eingabeaufforderung auf dem Sicherungsquellenknoten.
2. Führen Sie den folgenden Befehl aus, um die Anzahl von Datenträgern zu identifizieren, die die VM hat:

   ```
   ls /dev/xvd*
   ```
3. Führen Sie den folgenden Befehl aus, um den Algorithmus des Eingabe/-Ausgabe-Planer der Datenträger zu identifizieren:

   ```
   cat /sys/block/xvda/queue/scheduler
   ```

   Das folgende Ergebnis wird auf der VM angezeigt:

   ```
   [noop] anticipatory deadline cfq
   ```
4. Führen Sie den folgenden Befehl aus, um den Eingabe/-Ausgabe-Planer auf cfq zu ändern:

   ```
   echo "cfq" > /sys/block/xvda/queue/scheduler
   ```
5. Überprüfen Sie den Eingabe/-Ausgabe-Planer erneut.

   Das folgende Ergebnis wird auf der VM angezeigt:

   ```
   noop anticipatory deadline [cfq]
   ```
6. Ändern Sie den Eingabe/-Ausgabe-Planer für jeden Datenträger.
7. Führen Sie den Sicherungsjob erneut aus.

Der Sicherungsjob wird mit einem optimalen Sicherungs-Lesedurchsatz ausgeführt.

So stellen Sie die Vorgängerversion des Sicherungsservers wieder her

Gültig unter Red Hat Enterprise Linux (RHEL) 6.x und CentOS 6.x für Sicherungsserver

Problem

Beim Versuch, ein Upgrade des Sicherungsservers durchzuführen, tritt während des Upgrade-Vorgangs ein Fehler auf. Der Sicherungsserver funktioniert nicht erwartungsgemäß. Deswegen soll die Vorgängerversion des Sicherungsservers wiederhergestellt werden.

Lösung

Wenn Sie ein Upgrade auf eine neue Version durchführen, erstellt der Sicherungsserver einen Sicherungsordner, der alle alten Konfigurationsdateien und Datenbankdateien der zuvor installierten Version enthält. Der Ordner befindet sich im folgenden Speicherort:

```
/opt/CA/d2dserver.bak
```

Gehen Sie wie folgt vor:

1. Deinstallieren Sie den Sicherungsserver mit dem folgenden Befehl:

   ```
   /opt/CA/d2dserver/bin/d2duninstall
   ```

2. Installieren Sie die zuvor installierte Version des Sicherungsservers.
3. Halten Sie den Sicherungsserver mit folgendem Befehl an:

   ```
   /opt/CA/d2dserver/bin/d2dserver stop
   ```

4. Kopieren Sie die alten Konfigurationsdateien und Datenbankdateien mit dem folgenden Befehl in den Ordner "d2dserver":

   ```
   cp –Rpf /opt/CA/d2dserver.bak/* /opt/CA/d2dserver/
   ```

5. Starten Sie den Sicherungsserver mit folgendem Befehl:

   ```
   /opt/CA/d2dserver/bin/d2dserver start
   ```

Die zuvor installierte Version des Sicherungsservers wurde erfolgreich wiederhergestellt.

SLES 10.X startet nach einer BMR nicht erfolgreich

Gültig unter SUSE Linux Enterprise Server (SLES) 10.X für BMR auf alten Zielcomputern

Problem:

Bei der Ausführung einer BMR mit SLES 10.x-Wiederherstellungspunkten zu alten Zielcomputern ist die BMR ist erfolgreich, doch der Zielcomputer startet nicht erfolgreich. Bei der Ausführung einer BMR mit Wiederherstellungspunkten von einem alten SLES 10.x-Quellrechner ist die BMR ist erfolgreich, doch der Zielcomputer startet nicht erfolgreich.

In beiden den Fällen wird die folgende Fehlermeldung zurückgegeben:

```
No operating system (Kein Betriebssystem)
```

Lösung:

Ändern Sie den MBR des Startdatenträgers in einer Live-CD-Umgebung, und starten Sie den Zielcomputer neu.

Gehen Sie wie folgt vor:

1. Melden Sie sich mithilfe einer Live-CD beim Zielcomputer an, und suchen Sie den Startdatenträger.

   Beispiel: /dev/sda

2. Führen Sie folgenden Befehl aus:

   ```
   echo -en "\\x90\\x90"|dd of=/dev/sda seek=156  bs=1
   ```

3. Starten Sie den Zielcomputer neu, und stellen Sie sicher, dass der Zielcomputer erfolgreich neu startet.

Der SLES-10.x-Zielcomputer startet nach einer BMR erfolgreich.

d2drestorevm- und d2dverify-Jobs schlagen auf Oracle VM Server fehl

Gültig auf Oracle VM-Server

Problem

Wenn d2drestorevm- und d2dverify-Jobs auf Oracle VM Server gestartet werden, schlagen alle Jobs fehl. Im Aktivitätsprotokoll wird die folgende Fehlermeldung angegeben:

```
Das ISO-Image konnte nicht in den Hypervisor importiert werden.
Ausführlichere Informationen finden Sie in der
Hypervisor-Verwaltungskonsole oder im Debug-Protokoll.
```

Lösung

Überprüfen Sie, ob Oracle VM Server hängt.

Gehen Sie wie folgt vor:

1. Melden Sie sich Sie bei der Oracle VM Server-Konsole an, und navigieren Sie zur Registerkarte "Jobs".
2. Suchen Sie alle Jobs, die sich in Bearbeitung befinden, und brechen Sie diese Jobs ab.
3. Starten Sie den d2drestorevm- bzw. d2dverify-Job neu.

   Wenn der d2drestorevm- oder d2dverify-Job erneut fehlschlägt und die gleiche Fehlermeldung angezeigt wird, melden Sie sich Sie bei der Oracle VM Server-Konsole an, und überprüfen Sie, ob Jobs vorhanden sind, deren Status als in Bearbeitung angezeigt wird. Wenn Jobs vorhanden sind, deren Status als in Bearbeitung angezeigt wird, starten Sie diese Oracle VM Server-Instanz neu.

Die d2drestorevm- und d2dverify-Jobs werden erfolgreich ausgeführt.

Der virtuelle ESXi-Rechner kann nach einer BMR von einem physischen Rechner nicht gestartet werden

Symptom:

Ich führe eine BMR mithilfe von Wiederherstellungspunkten eines physischen Rechners auf einen virtuellen ESXi-Rechner aus. Der physische Rechner verwendet einen älteren BIOS. Die BMR ist erfolgreich, aber der virtuelle ESXi-Rechner wird nicht erfolgreich gestartet.

Lösung:

Ändern Sie den SCSI-Controller-Typ des ESXi-VM-Ziels, und übergeben Sie den BMR-Job erneut.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim ESX Server an.
2. Klicken Sie mit der rechten Maustaste auf das ESXi-VM-Ziel, und wählen Sie "Edit Settings" aus.
3. Wählen Sie auf der Registerkarte "Hardware" den SCSI-Controller 0 aus, und klicken Sie auf die Schaltfläche "Change Type".

   Das Dialogfeld "Change SCSI Controller Type" wird geöffnet.
4. Wählen Sie "LSI Logic SAS" aus, und speichern Sie die Einstellungen.
5. Übergeben Sie einen BMR-Job an diese VM.

Der virtuelle Rechner wird nach dem BMR-Job erfolgreich gestartet.